UNIVERSIDADE FEDERAL DE SANTA CATARINA
PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIA DA COMPUTAÇÃO

Wagner Tatsuya Watanabe

Desenvolvimento de um Modelo de Segurança no Gerenciamento de Contabilidade Baseado na Arquitetura TINA

Dissertação submetida à Universidade Federal de Santa Catarina como parte dos requisitos para a obtenção do grau de Mestre em Ciência da Computação.

Prof. Dr. Carlos Becker Westphall
Orientador

Florianópolis, Agosto de 2002

Desenvolvimento de um Modelo de Segurança no Gerenciamento de Contabilidade Baseado na Arquitetura TINA

Wagner Tatsuya Watanabe

Esta Dissertação foi julgada adequada para a obtenção do título de Mestre em Ciência da Computação - Área de Concentração SISTEMAS DE COMPUTAÇÃO e aprovada em sua forma final pelo Programa de Pós-Graduação em Ciência da Computação.

_____

Prof. Dr. Fernando Álvaro Ostuni Gauthier

Banca Examinadora

_____

Prof. Dr. Carlos Becker Westphall

_____

Profª Drª. Carla Merkle Westphall

_____

Prof. Dr. Arthur Ronald de Vallauris Buchsbaum

Dedico este trabalho ao meu orientador e co-orientador,
professores,
amigos,
e a todos os meus familiares.

Agradecimentos

Á Deus, pela minha vida e tudo que conquistei, meu Muito Obrigado.

Gostaria de agradecer aos professores integrantes da banca examinadora pela apreciação do presente trabalho.

Em especial, agradeço ao meu orientador, Dr. Carlos Becker Westphall, sua esposa Dra. Carla Merkle Westphall e a meu co-orientador Luis Marco Cáceres Alvarez, pelo empenho e dedicação a este trabalho e às suas atividades acadêmicas.

Finalmente, agradeço meus pais, fonte infinita de amor, carinho e compreensão.

Sumário

Lista de Figuras

Lista de Tabelas

Lista de Abreviaturas

3Pty : Third Party
5W : What, hoW, When, Who, Where
AccMgmtCtxt : Accounting Management Context
BrK : Broker
CC : Connection Coordinator
CO : Computational Objects
ConS : Connectivity Service
CORBA : Common Object Request Broker Architecture
CORBASEC : CORBA Security Services
CPE : Customer Premise Equipment
CSM : Communication Session Manager
DPE : Distributed Processing Environment
FCAPS : Failure, Configuration, Accounting, Performance and Security
GSEP : Generic Session End Point
GSM: : Global System for Mobile
IA : Initial Agent
IN : Intelligent Networks
IP : Internet Protocol
ISO : International Organization for Standardization
ITU : International Telecommunications Union
Ktn : Kernel Transportation Network
LNC : Layer Network Coordinator
LNFed : Layer Network Federation
NCCE : Native Computing and Communications Environment
ODP : Open Distributed Processing
PA : Provider Agent
PC : Personal Computer
PINT : PSTN and Internet Internetworking
PKI : Public Key Infrastructure

PSTN : Public Switched Telephone Network
QoS : Quality of Service
Ret : Retailer Reference Point
RMI : Remote Method Invocation
RM-ODP : Reference Model for Open Distributed Processing
RtR : Retailer to Retailer
SBS : Security Base Server
SF : Service Factory
SI : Security Interceptor
SMIB : Security Management Information Base
SSM : Service Session Manager
ST : Service Transaction
STR : Service Transaction Record
SUB : Subscription
Tcon : Terminal connection
TCSM : Terminal Communication Session Manager
TINA : Telecommunication Information Networking Architecture
TINA-C : TINA Consortium
TLA : Terminal Layer Adapter
TMN : Telecommunication Management Network
UA : User Agent
USM : Usage Session Manager
Vod : Vídeo on Demand
VoIP : Voice over IP

Resumo

O contínuo crescimento das redes de telecomunicações e das aplicações multimídia para a internet tem despertado interesse não só de pesquisadores, como também de profissionais da área de redes de computadores e de usuários em geral. Neste cenário, os fornecedores necessitam de mecanismos para se assegurarem que irão receber pelos serviços que estão disponibilizando, e os usuários também precisam ter a garantia de que pagarão exatamente pelo que solicitaram. Todos estes serviços e informações podem ser alvos de ataques, e estes ataques podem ser provenientes de dentro da própria rede ou por indivíduos externos a esta rede. Neste contexto, o TINAC (*Telecommunications Information Networking Architecture Consortium*) desenvolveu uma arquitetura detalhada para as redes de comunicação multi-serviço que permite o acesso às informações entre provedores e usuários em tempo-real, dentro de um ambiente seguro e confiável. Neste trabalho, será discutido as características e os requisitos de contabilidade e segurança dentro do contexto do gerenciamento de contabilidade. Um modelo para a segurança da contabilidade TINA é proposto utilizando os conceitos de segurança multilateral, o qual permite o estabelecimento de relações seguras entre os diversos participantes TINA. Por fim, um protótipo será implementado para validar os conceitos apresentados.

Palavras-chave

TINA, gerenciamento de contabilidade, gerenciamento de segurança, segurança multilateral.

Abstract

The continuous growth of the telecommunications networks and of the multimedia applications for the Internet has awake not only interest of researchers, as also of computer networks professionals in general. In this scene, the suppliers need mechanisms to make sure that they will receive for the services that they are offering, and the users also want the guarantee that they will pay accurately for what they had ordered. All these services and information can be a target of attacks, and these attacks can be proceeding from inside of the net or by external individuals. In this context, TINAC (Telecommunications Information Networking Architecture Consortium) developed a detailed architecture for the multi-service communication networks that allows the access to the information between suppliers and users in real-time, in a secure and trustworthy way. In this work, it will be argued the characteristics and the requirements of accounting and security inside the context of the accounting management. A model for security of TINA accounting is proposed using the concepts of multilateral security, which allows the establishment of safe relationships between several TINA participants. Finally, a prototype will be implemented to validate the concepts presented.

Key words

TINA, accounting management, security management, multilateral security.

1. Introdução

1.1. Visão Geral

Nos últimos anos, a estrutura de telecomunicações existente passou a ser utilizada como base para novos serviços de telecomunicações mais avançados e dinâmicos. Inicialmente, as redes eram utilizadas somente para a telefonia analógica, permitindo a comunicação instantânea entre pontos remotos. A crescente demanda por serviços de comunicação e o rápido avanço da informática conduziram à criação de complexas estruturas de redes de telecomunicações, onde predomina o tráfego de informações digitais como voz, imagens e dados.

O sucesso da Internet demonstra claramente o imenso potencial comercial dos serviços de comunicação. Os consumidores já conhecem os tipos de serviços que estão ao seu alcance ou que deveriam ser oferecidos pela infraestrutura de telecomunicações, principalmente se estes serviços oferecem suporte a diversos tipos de mídias (som e vídeo) e que sejam de fácil configuração. Os consumidores ainda esperam que estes serviços estejam disponíveis sob demanda, independente de sua localização ou de limitações de seu equipamento. Enquanto que boas partes dos componentes tecnológicos necessários já existam, ainda não existe consenso da melhor maneira de utilizá-los, de modo que vá de encontro às necessidades do volátil mercado (BRENNAN, 2000).

O conceito de Redes Inteligentes[1] (*IN–Intelligent Networks*) foi desenvolvido devido à necessidade de se disponibilizar rapidamente novos serviços de telecomunicações (PAVLOU, 1998). Como exemplos bem conhecidos de Redes Inteligentes pode-se citar o serviço de 0800 e o 0900.

[1] É um conceito arquitetural que provê a execução em tempo real de serviços de rede e de aplicações para usuários em um ambiente distribuído constituído por computadores e sistemas de comutação interconectados.

Para dar suporte e agregar novas funcionalidades a esta nova infraestrutura de redes, estruturas e arquiteturas de gerência como o TMN *(Telecommunication Management Network*) (ITU,1993) foram criadas e outras ainda estão em desenvolvimento, como o PINT (IETF,1999), Parlay (PARLAY,2001) e a TINA (TINA, 2000).

A Internet surgiu como uma grande aliada na era da multimídia. Seu desenvolvimento ocorreu de forma paralela com todo o desenvolvimento em telefonia e na telecomunicação tradicional. Eles usam diferentes tecnologias para fornecer diferentes características. Especificamente, a tecnologia da Internet emprega grande parte da inteligência nos terminais dos usuários, enquanto que no caso da telecomunicação tradicional, a inteligência se localiza principalmente dentro da própria rede. Quando integradas estas duas tecnologias podem oferecer uma vasta gama de oportunidades para prover versáteis serviços de informações e de multimídia além de inovar a maneira como estes serviços são criados e disponibilizados (TINA, 2000).

Neste contexto, a arquitetura TINA pretende estabelecer uma arquitetura baseada em tecnologias de computação distribuída que permitirá às redes de telecomunicações a introdução e o controle de novos serviços de uma maneira ágil e padronizada.

1.2. Objetivos Gerais

Este trabalho tem como principais objetivos:

- Estudar os principais conceitos relacionados à TINA.
- Estudar a Arquitetura de Contabilidade de TINA.
- Propor um modelo de segurança para o Gerenciamento da Contabilidade TINA
- Desenvolver um protótipo para a validação dos resultados esperados em nível de:
    - Gerenciamento de contabilidade, e
    - Gerenciamento de segurança.

1.3. Apresentação do trabalho

Este trabalho está organizado da seguinte maneira:

No Capítulo 2 são apresentados os conceitos básicos da arquitetura TINA, as subarquiteturas que a compõem, o Modelo de Negócios TINA e uma detalhada descrição da Arquitetura de Serviços, do conceito de Sessões e do Gerenciamento de Serviços.

O Capítulo 3 apresenta a gerência de contabilidade, as dificuldades e questões identificadas na gerência de contabilidade, a estrutura de informação *AcctMgmtCtxt* e como a gerencia de contabilidade se relaciona com a Transação de Serviço.

No Capítulo 4, questões relacionadas à segurança da arquitetura TINA são apresentadas, bem como uma análise das ameaças de segurança em diversos níveis de serviços oferecidos por TINA. Neste capítulo também são apresentados os conceitos da segurança multilateral.

No Capítulo 5 a proposta do modelo desenvolvido é apresentada. Os componentes que o constituem também são descritos.

O Capítulo 6 apresenta os resultados obtidos com a implementação do protótipo, as interfaces que foram geradas e um exemplo da execução do protótipo.

2. Arquitetura TINA – Conceitos Básicos

2.1 Introdução

A arquitetura TINA fornece uma arquitetura aberta na qual novos serviços e novas funcionalidades podem ser facilmente construídos e adicionados, diferente da maneira tradicional onde novos serviços são adicionados à rede de maneira não padronizada. Isto soluciona não somente o problema do desenvolvimento de novas aplicações, mas também o problema de interoperabilidade entre sistemas de diferentes fabricantes (NIEHAUS, 1999).

Estas características apresentadas de TINA permitem definir três importantes objetivos, que são:

a) Facilitar a distribuição de serviços de multimídia e de informações;
b) facilitar a criação e gerenciamento de novos serviços;
c) criar uma arquitetura aberta de componentes de telecomunicações e informações.

Desta maneira, o consórcio TINA (TINA-C) procura cumprir estes objetivos através da utilização dos mais recentes desenvolvimentos tecnológicos, incluindo redes de banda larga, diversas formas de comunicação existentes e principalmente as tecnologias Internet e Intranet, a qual TINA pretende contribuir com serviços tais como pontos de acessos e roteamento inteligente (NIEHAUS, 1999).

TINA é aplicável a todas as partes de um sistema de telecomunicações ou de informação:

- Terminais: computadores, pontos de acesso, etc.
- Servidores de transporte: *switches*, roteadores.
- Servidores de serviço: Web, VoD (*Vídeo-on-Demand*), VoIP (*Voice over IP*).
- Servidores de gerenciamento: autenticação, contabilidade e cobrança.

Para assegurar a interoperabilidade, portabilidade e reusabilidade dos componentes de software, é necessário existir uma independência de tecnologias específicas que

permitam o compartilhamento na criação e gerenciamento de complexos sistemas. Para isto, TINA é baseada em quatro princípios fundamentais:

1) Análise orientada a objetos: permite a divisão de um sistema em um conjunto de modelos que interagem.
2) Distribuição de componentes de serviço através da rede. Esta distribuição é suportada pelo Ambiente de Processamento Distribuído (*DPE - Distributed Processing Environment*).
3) O desacoplamento de determinados componentes de software não altera o funcionamento dos outros componentes.
4) A separação dos relacionamentos entre as partes do sistema permite que TINA forneça dois principais tipos de independência:
   - entre a aplicação e o ambiente na qual ele é executado;
   - independência da aplicação dentro de partes específicas do serviço e parte do gerenciamento e do controle.

A arquitetura de software TINA separa as aplicações de telecomunicações, ou seja, softwares que implementam as funcionalidades providas pelo sistema do DPE, que são softwares que suportam a execução distribuída de aplicações. Enquanto que as aplicações e o DPE são implementados como um conjunto de objetos que interagem, TINA não obriga o uso de uma linguagem de programação orientada a objetos para sua implementação. Uma vez que TINA não existe isoladamente, é preciso que se tenha a habilidade de interagir com sistemas não-TINA em um (ou ambos) nível(is) de serviço(s).

2.1.1 Arquitetura em Camadas

A arquitetura TINA é dividida em 4 camadas, como mostra a Figura 2-1. Iniciando pela camada do nível inferior, temos:

a) **Camada de Hardware**: envolve os processadores, memória, dispositivos de comunicação.
b) **Camada de Software**: envolve os sistemas operacionais, software de comunicações e outros softwares de suporte encontrados em recursos

computacionais. Esta camada é chamada também de Ambiente de Comunicação e Computação Nativa (*NCCE - Native Computing and Communications Environment*). O NCCE é composto de um conjunto de nós computacionais interconectados, onde cada nó pode suportar diferentes tecnologias de software e hardware.

c) **Camada DPE**: fornece suporte para a execução das aplicações de telecomunicações distribuídas, além de possuir uma visão independente da tecnologia dos recursos computacionais. Uma vez que as aplicações distribuídas são implementadas como um conjunto de objetos que interagem e que podem estar localizados em diferentes nós, o DPE provê suporte para a localização do objeto e interação remota.
d) **Camada de Aplicações**: implementa as funcionalidades oferecidas pelo sistema.

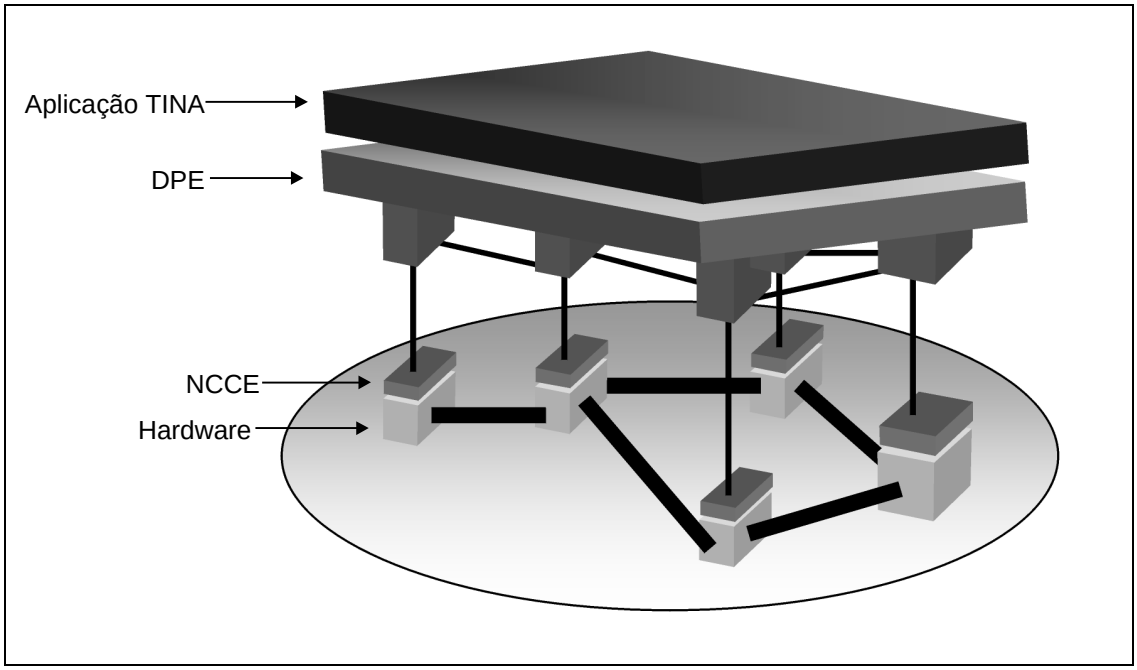

Figura 2-1: Arquitetura em camadas TINA (NIEHAUS, 1999).

O sistema TINA em camadas consiste de nós separados na qual cada nó possui um NCCE e um DPE. A junção de todos os DPEs forma uma “superfície DPE”, onde cada nó pode ser de propriedade de diferentes Administradores, Consumidores e Provedores de Serviço. A interface inter-DPE é definida em comum acordo entre todos os fabricantes ou por um padrão.

2.1.2 A Arquitetura TINA

A arquitetura TINA é dividida em quatro sub-arquiteturas. Os relacionamentos entre estas quatro arquiteturas são demonstrados na Figura 2-2 e explicados a seguir:

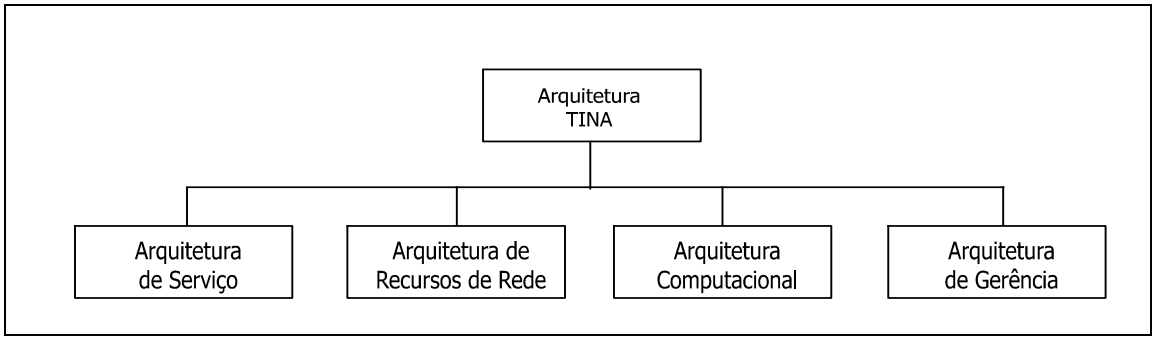

Figura 2-2: Sub-Arquiteturas TINA (NIEHAUS, 1999).

1) **Arquitetura de Serviço**: consiste de um conjunto de conceitos, princípios, regras e padrões (*guidelines)* para a construção, desenvolvimento e operação dos serviços TINA.
2) **Arquitetura de Recursos de Rede**: estabelece um conjunto de conceitos que descrevem as redes de transporte de uma maneira independente da tecnologia e provê mecanismos para o estabelecimento, modificação e liberação de conexões de rede (estes mecanismos são definidos como um conjunto de interfaces disponíveis para a camada de Recursos de Rede), (ABARCA, 1997).
3) **Arquitetura Computacional**: define os conceitos de modelagem orientada a objetos e o Ambiente de Processamento Distribuído (DPE) que fornece ao sistema o meio para que objetos possam se localizar e interagir. Estes conceitos estão baseados no RM-ODP (Reference Model for Open Distributed Processing) (ISO, 1994).
4) **Arquitetura de Gerência**: especifica os princípios e conceitos gerais de gerenciamento para a arquitetura TINA. Estes conceitos são derivados dos padrões (ITU, 1993).

2.2 O Modelo de Negócios TINA

O Modelo de Negócios define um *framework* para especificar Pontos de Referência[2] e propagar requisitos em TINA. O Modelo de Negócios provê a estrutura para especificar, adicionar e modificar Pontos de Referência e componentes em TINA (MULDER, 1997).

Em TINA a implementação da arquitetura de serviço e da arquitetura de recursos de rede são aplicações executadas em um ambiente DPE. As especificações dos Pontos de Referência descrevem as interações entre estas aplicações e a plataforma DPE em todos os aspectos de TINA.

Na Figura 2-3 é ilustrado o Modelo de Negócios utilizado em TINA. Este modelo mostra cinco "áreas-chaves" (Funções de Negócios) com seus relacionamentos identificados. Estes relacionamentos no Modelo de Negócios são usados para identificar e definir os Pontos de Referências (por ex. *Bkr*, *Ret*, *Tcon*, *3Pty*, etc) das aplicações.

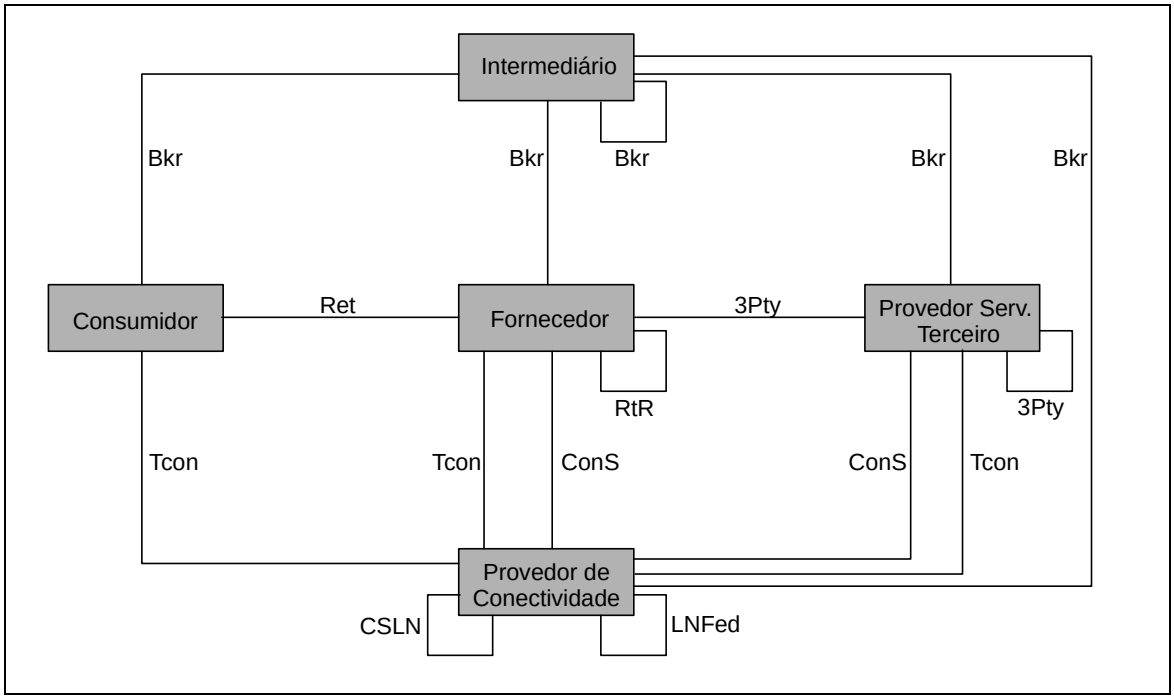

Figura 2-3: Componentes (*Business role*) e tipos de relacionamentos TINA (MULDER, 1997).

[2] Um Ponto de Referência define um conjunto de interfaces associado com o modelo o qual é considerado potencialmente adequado para uma plataforma DPE.

2.2.1 Escopo do Modelo de Negócios

O Modelo de Negócios em TINA especifica:

- Um *framework* de negócios genérico para todos os integrantes da TINA. Ele define um conjunto de condições na qual os seguintes ítens podem ser realizados:
  - A criação de novas funções de negócios e Pontos de Referência, estas novas funções podem interagir com os já existentes.
  - A melhoria de funções de negócios e Pontos de Referências existentes para agregar novas regras e funcionalidades usando Pontos de Referências já definidos e implementados.
- Um conjunto inicial de funções e relacionamentos de negócios para aplicar em TINA, utilizando *drivers* de Serviços de Telecomunicações e Serviços de Informações já existentes no mercado.
- Requisitos impostos a TINA para atender a um conjunto específico de serviços, e propagando estes requisitos nas funções e relacionamentos de negócios nos Pontos de Referências dos participantes TINA proprietários do sub-sistema.

2.2.2 Definição do *Framework*

A base dos sistemas e subsistemas TINA é constituída pelos objetos de informações, objetos de computação e objetos de engenharia sob um Domínio Administrativo de Negócios e separados por Pontos de Referências. Desta maneira, a especificação de regras e interações entre Domínios de Gerência TINA se propagam através da especificação da visibilidade e direitos em cada tipo de objeto nos domínios relacionados. Estes direitos e visibilidades são colocadas em um contrato. Um contrato é um contexto definindo as restrições aonde o(s) ponto(s) de referência(s) irá(ão) operar. O contrato é estabelecido entre domínios de gerência de negócios e pode ser negociado *on-line* ou *off-line*.

2.2.3 Contrato

O Contrato provê a base para os contextos definidos em outros *viewpoints*[3]. Com as restrições definidas no contrato, os contextos em outros *viewpoints* podem ser negociados *on-line* ou *off-line*. Entretanto, o contrato nunca pode ser modificado como resultado de negociações em outro *viewpoint*, uma vez que um simples *viewpoint* somente provê uma visão parcial das interações entre os Domínios Administrativos de negócios e pode violar as políticas negociadas para outros *viewpoints*.

2.2.4 Domínio Administrativo de Negócios

Um Domínio Administrativo de Negócios é definido pelos requisitos de um *business role*. Um Domínio Administrativo de Negócios irá interagir com outro através dos Pontos de Referência, os quais são as implementações dos relacionamentos de negócio.
Para permitir a interação entre os Domínios Administrativos de Negócios, eles devem possuir um Ponto de Acesso, isto é, um objeto que aceite requisições de serviços provenientes de outros componentes. Informações sobre estes acessos são registradas e gerenciadas pelo *broker*[4] de negócios.
O conceito de Domínio Administrativo de Negócios é baseado em *propriedades*, partindo do ponto de vista da empresa. A propriedade implica em um privilégio dominante na gerência de entidades dentro do domínio. Este privilégio pode ser delegado para domínios em outros *viewpoints*. Por exemplo, o Domínio de Gerência no *viewpoint* da informação pode resolver um problema específico (p. ex no gerenciamento de falhas) ou um relacionamento como no gerenciamento de rede de uma rede particular de propriedade de um Domínio de Gerência de Negócios, (Figura 2-4). Em outras

---

[3] Uma forma de abstração alcançada usando um conjunto selecionado de conceitos de arquiteturas e regras de estruturação de maneira a focalizar um interesse em particular em um sistema. TINA provê conceitos de arquitetura para *viewpoints* de informação, computacional e de engenharia.

[4] É um *business role* que provê informações sobre como encontrar certos serviços e certos participantes em TINA.

visões o Domínio Administrativo de Negócios pode ser dividido e agregado em outros tipos de domínios de maneira a facilitar a solução de problemas e relacionamentos.

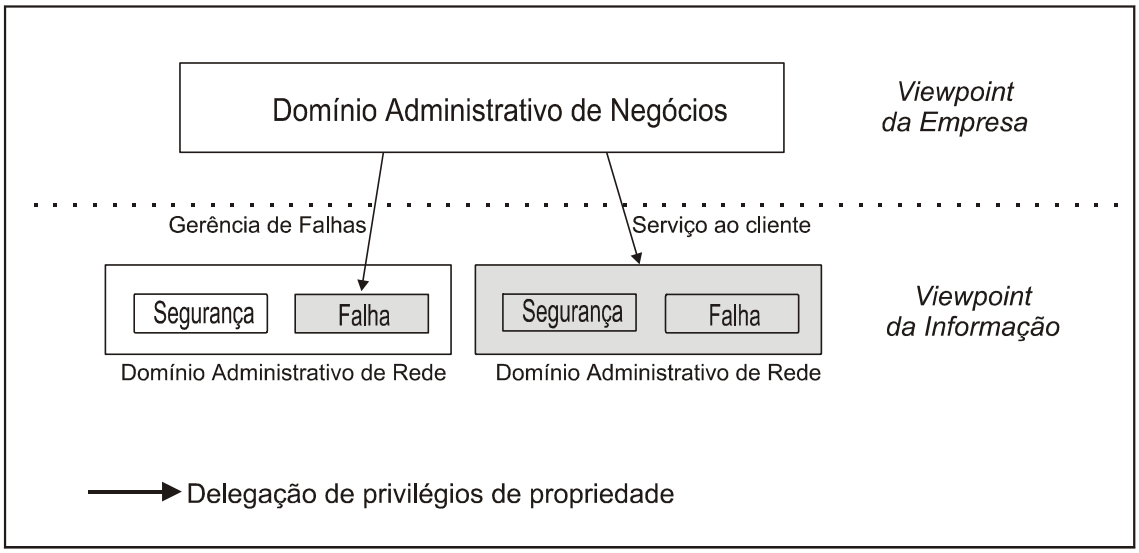

Figura 2-4: Mapeamento de Domínios (MULDER, 1997).

2.2.5 Pontos de Referência

O Ponto de Referência é composto por diversas especificações de *viewpoints* relacionados por um contrato, com o propósito de favorecer a reutilização e a implementação modular das especificações. O Ponto de Referência contém os seguintes segmentos:

1. **Segmento de negócios:** limitações de escopo, requisitos funcionais e não-funcionais atribuídos aos relacionamentos de negócios pelos componentes. Ele é derivado a partir dos requisitos dos componentes e suas interações.
2. **Segmento de informações:** define a informação a qual é compartilhada entre os Domínios de Gerência de Negócios.
3. **Segmento computacional:** define as interfaces em objetos computacionais de maneira a serem acessíveis para outros domínios.
4. **Segmento de engenharia:** define a separação do DPE em nós DPE, *Ktn links* (*kernel Transportation Network*) e pilhas de protocolos necessários para a interoperabilidade entre os Domínios Administrativos de Negócios.
5. **Segmento de miscelânea:** define outras restrições como as limitações das especificações importadas para a especificação do Ponto de Referência.

2.2.6 Participantes[5]

Um conjunto inicial de componentes na arquitetura TINA foi identificado através da análise dos relacionamentos de negócios atualmente existentes nas telecomunicações e serviços de informações, como ilustrado na Figura 2-3. A seguir define-se cada um dos participantes.

a) Consumidor (*Consumer*)

Um participante com a Função de Negócios **Consumidor** usufrui as vantagens dos serviços fornecidos por TINA. Este tipo de participante é a base econômica da TINA, uma vez que será ele quem irá pagar pela utilização dos serviços TINA. O perfil dos participantes com a função de negócios Consumidor é variável, podendo variar desde grandes empresas ou corporações a usuários individuais, em caso similar aos usuários da Internet.

Os requisitos de alto nível para esta Função de Negócio em TINA são:

- Obtenção da localização de Fornecedores, Provedores de Serviços, e outros Consumidores.
- Registro e cancelamento de registro dos Fornecedores.
- Inicialização de relacionamentos de serviços que incluam os Provedores de Serviços e outros Consumidores.
- Sinalização de disponibilidade para os Fornecedores (para a recepção de convites).
- Aceitar convites para ingressar em sessões de outros Consumidores ou Fornecedores.
- Aceitar *downloads* de Fornecedores para a atualização da capacidade de interação com o Fornecedor (*upgrades*).

[5] Pode ser um participante de qualquer tipo, empresa ou uma pessoa a qual possui uma porção (um ou mais domínios administrativos) em um sistema TINA.

b) Fornecedor (*Retailer*)

O participante na Função de Negócios **Fornecedor** provê serviços para os componentes na Função de Negócios Consumidor. O número de Fornecedores que podem estar relacionados em TINA pode variar de alguns Fornecedores até milhares de Fornecedores.

Um Fornecedor pode desenvolver um novo serviço para uso imediato por qualquer Consumidor em TINA, sem uma prévia autorização/padronização de outros Fornecedores. Isto permite um rápido desenvolvimento de aplicações e faz com que TINA seja um sistema dinâmico para a integração de novas aplicações.

c) Broker

O participante na Função de Negócios ***Broker*** possui a missão de prover informações que possibilitem que um participante encontre outros participante*s* ou serviços em TINA.

Em um sistema distribuído como TINA, existe a possibilidade de que qualquer participante possa estabelecer um contato lógico com qualquer outro participante. A obtenção de informações e endereços de outros participante*s* são suportados por mecanismos genéricos do *broker*, isto é, o *broker* provê o serviço para se encontrar um objeto requisitado em TINA.

d) Provedores de Serviços Terceirizados (*Third Party Service Provider*)

O objetivo de um participante com a Função de Negócios **Provedor de Serviços Terceirizados** é dar suporte em serviços para os Fornecedores ou outros Provedores de Serviços Terceirizados. Estes serviços podem ser considerados como “Serviços Negociáveis”. O Provedor de Serviço Terceirizado pode ser um servidor lógico ou servidor de dados ou ambos.

A diferença entre o Provedor de Serviço Terceirizado e um Fornecedor é de que o Provedor de Serviço Terceirizado não possui um vínculo contratual com os componentes na função de Negócios Consumidor. Entretanto, um participante pode se tornar um Fornecedor ou um Provedor de Serviço Terceirizado simultaneamente.

e) Provedor de Conectividade (*Connectivity Provider*)

O participante na Função de Negócio de **Provedor de Conectividade** gerencia a rede (switches, roteadores, links, etc). Esta rede pode constituir a rede de transporte que oferece suporte a ligações de fluxo ou podem constituir a rede de transporte de *kernel* para suportar ligações computacionais em TINA, provendo conexões entre nós de ambientes de processamento distribuídos.

A rede de transporte de um provedor de conectividade não é uma rede global que conecta todos os Consumidores, Fornecedores e Provedores de Serviços Terceirizados em um sistema TINA. A rede de transporte global é segmentada em diversas sub-redes controladas por diferentes componentes. O gerenciamento de conexões de cada um destes segmentos fica a cargo de certos Domínios Administrativos de Negócios. Para permitir a gerência das conexões roteadas através de dois ou mais segmentos de rede junto a diferentes provedores de conectividade, os provedores de conexão devem ser organizados entre si.

2.2.7 Relacionamentos de Negócios (Business relationship)

Para permitir que os cinco tipos de funções de Negócios anteriormente descritos possam interagir, um conjunto de tipos de Relacionamentos de Negócios foi definido. Alguns relacionamentos aparecem mais que outros (Figura 2-3), denotando múltiplas ocorrências do mesmo tipo de Relacionamento de Negócios entre diferentes funções de negócios. Entretanto, apesar dos tipos de funções de negócios e as interações serem os mesmos, as informações enviadas podem ser completamente diferentes.

A seguir são listadas as interações que devem ser executadas antes que quaisquer outras interações sejam iniciadas:

- Iniciar o diálogo entre os Domínios de Gerência de Negócios;
- identificar os Domínios Administrativos de Negócios entre as partes;
- estabelecer/liberar e gerenciar uma associação segura;
- descoberta de serviços e inicialização;
- estabelecimento do contexto de gerenciamento inicial; e

- negociação da utilização inicial de interações.

A seguir são descritas as interações genéricas para todos os Relacionamentos de Negócios, que permitem o suporte para o estabelecimento de relacionamentos gerenciáveis entre Domínios de Gerência de Negócios.

1. **Relacionamento de Negócios do Fornecedor** (*Ret - Retailer Business relationship*): o Relacionamento de Negócios *Ret* é utilizado entre participante com funções de Negócios Consumidor e participantes com funções de Fornecedor (FARLEY,1998).
2. **Relacionamento de Negócios do Intermediário** (*Brk - Broker business relationship*): o Relacionamento de Negócios *Brk* provê acesso às informações de gerência controladas por qualquer outra função de Negócios TINA. O *broker* pode prover diferentes tipos de informações para diferentes funções de Negócios e com finalidades diferentes.
3. **Relacionamento de Negócios Terceirizado** (*3Pty - Third Party business relationship*): um participante que possui a função de Negócios Fornecedor pode interagir com um participante que possui a função de negócios terceirizada para que possa fornecer uma grande variedade de serviços a seus consumidores sem ser realmente proprietário destes serviços.
4. **Relacionamento de Negócios Fornecedor para Fornecedor** (*RtR - Retailer to Retailer business relationship*): o Relacionamento de Negócios *RtR* reutiliza a funcionalidade dos Relacionamentos de Negócios *3Pty* e *Ret* considerando o fato de que as informações que trafegam neste relacionamento podem ser diferentes, mas as interações não são diferentes.
5. **Relacionamento de negócios de Serviços de Conectividade** (*ConS - Connectivity service business relationship*): o Relacionamento de Negócios *ConS* é definido entre o Provedor de Conectividade, fornecendo os serviços de transporte de rede e as funções de negócios usando os serviços de conectividade de transporte. As conexões são estabelecidas entre Pontos de Acessos de Redes arbitrários na camada de recursos de rede de TINA.

6. **Relacionamento de Negócios de Conexão de Terminais** (*Tcon - Terminal connection business relationship*): o Relacionamento de Negócios *TCon* provê a ligação de gerência entre a função de negócios do Provedor de Conectividade e as funções de negócios das partes envolvidas na Interface de Conexões Físicas (*Physical Connection Graph*). O relacionamento *TCon* está intimamente relacionado com o relacionamento *Ret* ou com o relacionamento *3Pty* a qual executa a liberação da conexão. Uma vez que os Pontos de Terminação de Rede (*Network Termination Points*) são dependentes da tecnologia, a implementação de interações do relacionamento *TCon* também serão dependentes da tecnologia.
7. **Relacionamento de Negócios da Camada de Redes Federativa** (*LNFed*: *Layer network federation business relationship*): o Relacionamento *LNFed* é um relacionamento federativo entre provedores de conectividade.
8. **Relacionamento da Camada de Rede Cliente-Servidor** (*CSLN*: *Client-server layer network relationship*): o relacionamento *CSLN* permite o uso de camadas entre Domínios de Gerência de Negócios executando funções de Provedores de Conectividade.

2.3 Arquitetura de Serviços TINA

A arquitetura de serviços TINA consiste de um conjunto de conceitos, princípios, regras e padrões para a construção, desenvolvimento e operação dos serviços TINA. O comportamento dos elementos em uma arquitetura TINA é modelado por componentes que operam em um Ambiente de Processamento Distribuído (DPE) e que interagem através de interfaces (KRISTIANSEN, 1997). A arquitetura de serviços TINA identifica os componentes para se elaborar serviços e também descreve a maneira como eles serão combinados e de que maneira devem interagir. A arquitetura de serviços também examina quais componentes são necessários em um ambiente para instanciar, gerenciar e utilizar os serviços.

2.3.1 Definição de Serviço

O termo serviço é usado em múltiplos sentidos. Uma definição tipicamente usada é que serviço é um conjunto de funções úteis oferecidos por um Provedor de Serviço para um consumidor. Na indústria de telecomunicações, um serviço pode ser visto como um conjunto "encapsulado" de capacidades que é percebido por um usuário humano quando interage com uma rede de Telecomunicações ou com um provedor de serviço e pela qual é realizada uma cobrança por este serviço.

Um serviço TINA é um conjunto de capacidades úteis fornecidas por um sistema existente para todas funções de negócios que o utilizem; cada função de negócios pode ver um mesmo serviço sob diferentes perspectivas.

Em TINA temos pelo menos estes três tipos de serviços (KRISTIANSEN, 1997):

- **Serviços de Telecomunicação**: São serviços baseados no transporte de bits de informações entre terminais conectados a uma rede de Telecomunicações. O Serviço de Telecomunicações é responsável pelo estabelecimento de conexões e pelo processamento das informações relacionadas com as conexões. A rede de Telecomunicações é transparente para as informações que trafegam entre os pontos da rede.
- **Serviços Gerenciáveis**: são serviços responsáveis pelo gerenciamento dos recursos TINA. Inclui funcionalidades de Falha, Configuração, Contabilidade, Performance e Segurança, assim como o serviço de gerência do ciclo de vida e o serviço de gerência de instância.
- **Serviços de Informações**: são serviços capazes de manipular informações de recursos como vídeo, sons ou documentos. Inclui o armazenamento (conteúdo) e a visualização (aplicações capazes de interpretar estes recursos). Também compreende os serviços necessários entre o armazenamento e a visualização tais como cobrança, *buffer* e todos os serviços específicos.

2.3.2 Ambiente Comercial da Arquitetura de Serviço

O principal objetivo da Arquitetura de Serviço é de suportar o mais geral dos casos de interação entre domínios de gerência de negócios através de um DPE de maneira a

oferecer objetos de negócios para a captação de receita. Um exemplo deste ambiente comercial é a seguir na Figura 2-5. O domínio administrativo de negócios “A” deseja fazer uso de uma aplicação oferecida por um outro domínio administrativo “B”. A aplicação pode ser totalmente fornecida por “B” ou “B” pode subcontratar esta aplicação (totalmente ou parcialmente) através de um ou vários domínios administrativos de gerência “C” e “D” (terceiros), cada um provendo contribuições únicas e diferentes para satisfazer “A”. Os domínios “C” e “D” podem ou não interagir diretamente com “A”. Estas interações representam os relacionamentos de negócio, onde a natureza e o ganho comercial de cada parte é único para cada aplicação e ocasião específica.

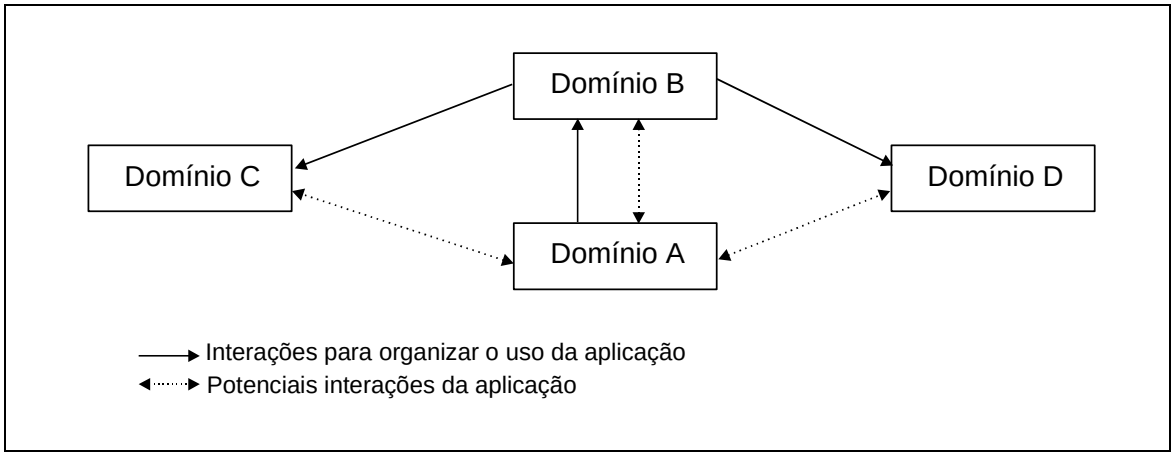

Figura 2-5: Exemplo de interações da arquitetura de serviços entre domínios administrativos de negócios (KRISTIANSEN, 1997).

2.3.3 Divisão entre Acesso, Serviço e Comunicação

A arquitetura de serviço é dividida em dois conceitos: *acesso* e *uso*. As interações necessárias para a descoberta e requisições de serviços são tratadas pelo *acesso*, enquanto que o controle do serviço e o envio do fluxo de conteúdo são tratados pelo *uso*. A figura 2-6 ilustra a divisão da arquitetura.

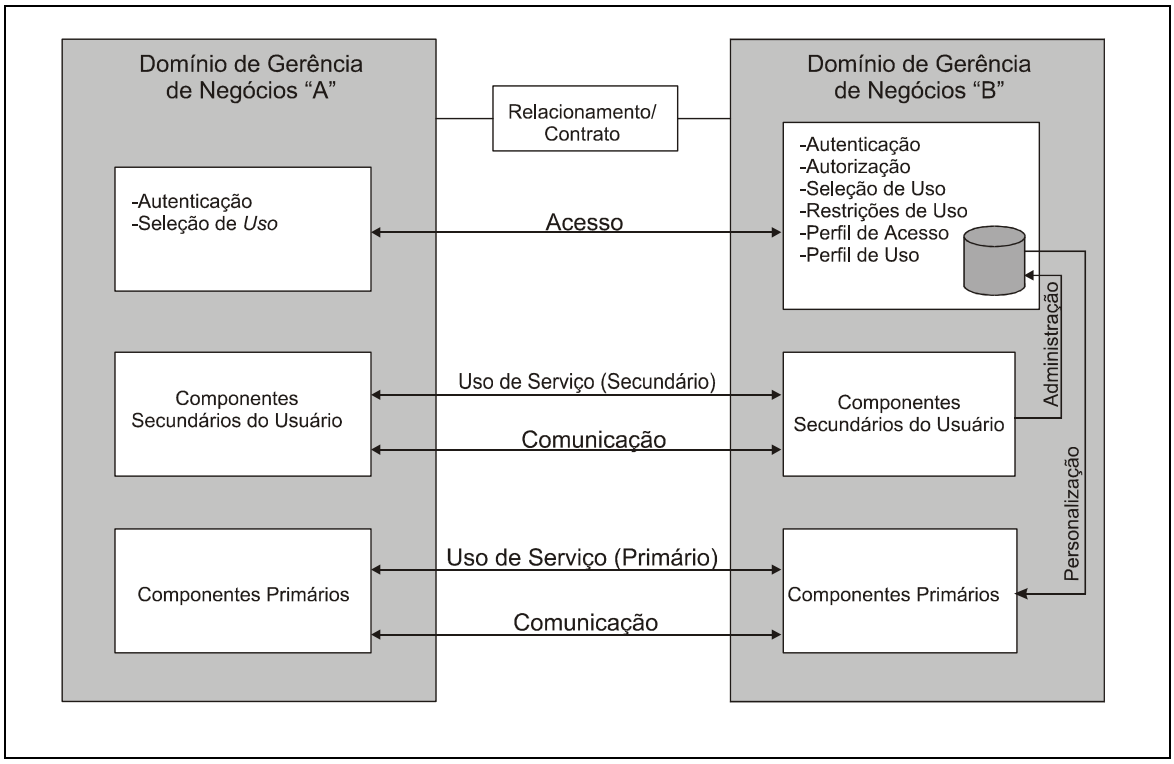

Figura 2-6: Acesso, uso primário e uso secundário (KRISTIANSEN, 1997).

a) O Acesso

O *acesso* trata das interações necessárias para se estabelecer a comunicação entre os dois domínios. No exemplo da Figura 2-6, "B" armazena informações sobre "A", como autorizações e preferências já conhecidas. A funcionalidade de *acesso* é definida de maneira simples para permitir a fácil implementação em equipamentos TINA para o mercado. Todas as outras interações são manipuladas como *uso*.

b) O Uso

O uso divide-se em:

- **Serviço**: As interações entre os componentes são necessárias para o controle do comportamento do serviço, como a troca de dados (conteúdo) e a manipulação de informações de gerenciamento.
- **Comunicação**: As interações de comunicação são necessárias para estabelecer e manter conexões entre componentes que implementam o serviço. Também são tratadas a negociação de QoS e a configuração e modificação de conexões.

c) *Uso* de serviço secundário

O serviço secundário é composto por interações de componentes desenvolvidos pelo provedor e que permitem ao cliente personalizar a apresentação e a utilização de componentes do provedor. Os limites do contrato do cliente são previamente estabelecidos entre as partes. Apesar dos serviços secundários não estarem implicitamente incluídos no contrato, eles agregam valores ao serviço primário.

d) *Uso* de serviço primário

O serviço primário trata de satisfazer o objetivo primário do contrato entre os dois domínios, como por exemplo uma conferência multimídia, a provisão de informações de um recurso ou um serviço de gerenciamento.

2.4 Sessões

Em TINA uma sessão é definida como:

- Um relacionamento temporário entre um grupo de objetos associados coletivamente para executar uma tarefa durante um período de tempo.
- Uma sessão possui um estado que pode mudar durante o seu tempo de vida.
- Uma sessão representa uma visão abstrata e simplificada do gerenciamento e uso de objetos e de suas informações compartilhadas.
- Os objetos em uma sessão estão sujeitos a políticas comuns que governam a sessão, alguns objetos podem estar sujeitos a aspectos derivados destas políticas.
- Uma sessão pode abranger múltiplos Domínios de Gerência de Negócios.
- O domínio da sessão define a política de um determinado domínio, e objetos computacionais e informações que estão sujeitos a tal domínio de sessão.

Na Figura 2-7 é representado o escopo das sessões em TINA. Na figura é representado um exemplo onde o Consumidor interage com outro participante em uma sessão de serviço oferecido por um Fornecedor e cujas funções principais são:

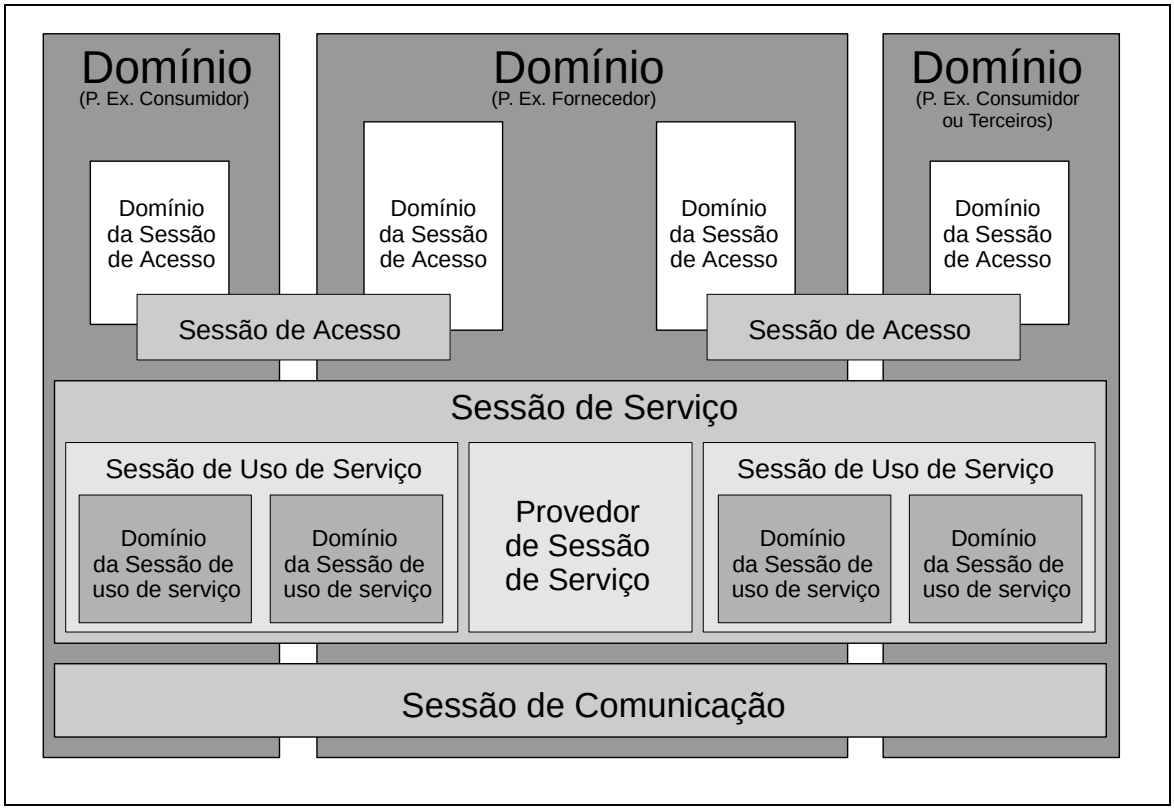

Figura 2-7 Exemplo de sessões TINA (KRISTIANSEN, 1997).

a) Sessão de Acesso

A Sessão de Acesso é estabelecida quando dois Domínios da Sessão de Acesso são interconectados em um relacionamento seguro. O próximo estágio da Sessão de Acesso é a negociação dos termos entre os domínios para que se continue a interação e a autenticação. A partir de uma Sessão de Acesso muitas Sessões de Serviço podem ser invocadas, a qual é responsabilidade da Sessão de Acesso gerenciar estas sessões até que a Sessão de Serviço termine ou seja associada a uma outra Sessão de Acesso (KRISTIANSEN, 1997).

b) Sessão de Serviço

Existem dois tipos de sessões de serviço:

- **Sessão de Serviço**: representa as informações e funcionalidades relacionadas aos serviços de execução, de controle e de gerência. Estes serviços incluem serviços primários (ex. conferência multimídia) e serviços secundários (ex. assinatura de um serviço on-line).
- **Provedor de Sessão de Serviço**: representa o centro do serviço lógico e de controle de um ou mais domínios que estejam participando do serviço.

c) Sessão de Comunicação

A Sessão de Comunicação representa uma visão geral do serviço de conexão e uma visão de rede independente da tecnologia e dos recursos necessários para se estabelecer uma conexão fim a fim. Uma sessão de comunicação pode manipular múltiplas conexões. Estas conexões podem ser multiponto (videoconferência) e/ou multimídia (imagem e som).
A adoção do conceito de “sessão” para o controle das comunicações possui a vantagem de permitir que os serviços sejam instanciados dinamicamente e manipulados para manter uma configuração adequada dos recursos de comunicações desejados.

2.5 Gerenciamento de Serviço

O Gerenciamento de Serviço é uma parte importante da arquitetura de serviço TINA. O gerenciamento de serviço envolve funções de gerenciamento e controle das transações fim-a-fim dos serviços TINA, as quais são fornecidas pelas propriedades FCAPS ditadas pelo contexto de gerenciamento de conexão. Os quatro conceitos associados com o gerenciamento de serviço são:

- **Conceito de Particionamento**: o gerenciamento de serviço TINA é particionado em três camadas: serviços, recursos e o DPE.
- **Conceito Funcional**: é mais bem representado pelas funções FCAPS. Para suportar integralmente as funções FCAPS, construções como gerenciamento de contexto e transações de serviços são fornecidos.

- **Conceito Computacional**: representa o suporte computacional para as necessidades de gerenciamento. O maior parte deste suporte computacional é fornecido pelo DPE.
- **Conceito de Ciclo de Vida**: representa questões relacionadas ao tempo de execução de uma determinada operação, tais como o ciclo de vida do serviço e o ciclo de vida do gerenciamento.

2.5.1 Aspectos Funcionais

O escopo funcional considera as capacidades que o gerenciamento de serviço pode assumir. TINA encobre as áreas de gerenciamento FCAPS, a seguir descritos (KRISTIANSEN, 1997):

- **Gerência de Falhas**: trata de alarmes de falhas em geral e também a correlação e distribuição de alarmes. Este tipo de gerenciamento é particularmente importante para que TINA seja confiável e tolerante a falhas, uma vez que consiste na maior parte de elementos distribuídos semi-autônomos. Esta mesma natureza distribuída dificulta muito o controle e a gerência de falhas no sistema.
- **Gerência de Configuração**: trata da configuração de recursos tais como recursos de rede, recursos computacionais, recursos de software, etc, para que os recursos configurados se tornem disponíveis para os serviços TINA. Como os tipos de recursos em TINA são muito diversos, a gerência de configuração em TINA é uma coleção de esquemas de gerenciamento para diferentes tipos de recursos.
- **Gerência de Contabilidade**: trata de questões como cobrança, objetos contábeis, e o envio de eventos de contabilidade. TINA possui opções flexíveis de contabilidade, como a cobrança on-line e cobrança por terceiros.
- **Gerência de Performance**: trata da monitoração, controle e administração da performance em TINA.
- **Gerência de Segurança**: trata de questões de segurança em nível de serviço, e subseqüentemente com todos os componentes que se situam no nível de recursos. A gerência de segurança TINA trata de questões como autenticação e autorização em um ambiente de domínio multi-provedor. A fim de estabelecer

uma sessão de serviço em um ambiente multi-provedor, uma rede de confiança precisa ser mantida e gerenciada apropriadamente entre os domínios.

2.5.2 Aspectos computacionais

A arquitetura TINA adotou o conceito de *viewpoints* ODP, incluindo os *viewpoints* computacional e de informações. O *viewpoint* computacional considera um sistema como um conjunto de objetos que interagem e que podem ou não ser distribuídos. Como TINA é baseado em uma arquitetura DPE, o aspecto computacional é muito importante. Ele provê a base para a estrutura do sistema gerenciado e de sistemas de gerência (KRISTIANSEN, 1997).

Um DPE oferece uma grande variedade de serviços de suporte para se manter um sistema de gerenciamento. Isto inclui vários serviços de gerenciamento de ciclo de vida que suportam: a criação e destruição de objetos; serviços de segurança como criptografia, autenticação e autorização; e outras funcionalidades como gerenciamento de eventos e *log*.

2.5.3 Aspectos de Informações.

Os aspectos de informações são definidos como:

a) Domínios

A arquitetura TINA não supõe que um simples provedor de serviço seja o responsável para fornecer todos os serviços, muito pelo contrário, é assumido que irá existir um número considerável de participantes atuando em diversas funções de negócios. Participantes são na realidade entidades comerciais que provêem serviços ou recursos de comunicações.

Para suportar um ambiente de múltiplos participantes, a arquitetura TINA reconhece o conceito de domínios. Estes podem ser Domínios de Gerência que são controlados por vários componentes. Com um Domínio Administrativo, vários Domínios de Gerência podem existir para auxiliar na organização de atividades de gerência necessárias.

b) Domínios de Gerência

Um Domínio de Gerência é modelado como um objeto de informação associado a certas funcionalidades de gerência como contabilidade, segurança ou gerência do DPE. Algumas das características do domínio de gerência são:

- Os limites dos domínios são geralmente baseados na afinidade natural dos objetos, como a topologia da rede, componentes de negócios ou área geográfica.
- Um domínio pode ser decomposto em subdomínios, permitindo uma composição hierárquica.
- Um objeto pertencente a um domínio também pode fazer parte de um outro domínio, estes podem estar relacionados de diversas maneiras.
- O comportamento dos objetos gerenciados e dos objetos gerenciadores em um domínio é regido por políticas de gerência que são aplicados no domínio.

c) Contexto de Gerenciamento

O contexto de gerenciamento representa um conjunto de requisitos e de funcionalidades para uma sessão com respeito a uma específica área de gerenciamento funcional. No Contexto de Gerenciamento são definidas as regras que serão utilizadas numa área, em particular de gerência funcional durante uma sessão. A área funcional de gerenciamento do contexto de gerência é associada a uma das áreas FCAPS, DPE ou ao gerenciamento do ciclo de vida.

O contexto de gerência de uma certa sessão é normalmente negociado por componentes em diferentes Domínios Administrativos. Um componente pode executar a função de provedor, enquanto que outros componentes podem executar a função de usuário.

2.6 Conclusão

Neste capítulo foi apresentado com detalhes a arquitetura TINA, as subarquiteturas que a compõe e suas funcionalidades. Os documentos do TINAC descrevem as arquiteturas com um alto grau de detalhamento, neste capítulo foram apresentadas somente as informações mais estreitamente relacionadas com a gerência de contabilidade em TINA

No capítulo seguinte a Arquitetura de Contabilidade TINA será detalhadamente explanada.

3. Arquitetura da Contabilidade TINA

3.1 Introdução

O objetivo da Arquitetura da Contabilidade TINA é prover uma contabilidade flexível e confiável com a adição de funcionalidades que não existem nas arquiteturas de contabilidade tradicionais. A gerência de contabilidade consiste de quatro ciclos como mostra a Figura 3-1 e que serão explicadas a seguir (HAMADA, 1996):

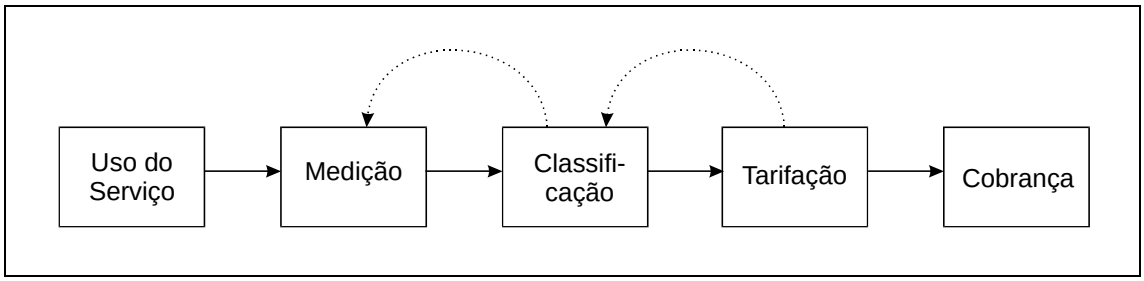

Figura 3-1 Ciclo Básico da Contabilidade (HAMADA, 1996).

a) **Medição**: trata da monitoração e do registro da utilização dos recursos. Devido à natureza distribuída de TINA, este tipo de tarefa enfrenta muitas dificuldades, pois os objetos e recursos encontram-se distribuídos e muitas vezes migram de um local para outro. A medição é o primeiro passo e a base de todas as atividades da contabilidade.
b) **Classificação**: classifica as informações da medição em um conjunto de classes baseado na utilização dos serviços, dos recursos que estão sendo utilizados, da distância entre o usuário e o provedor, etc. A finalidade da classificação é categorizar e reduzir a quantidade de informações da medição.
c) **Tarifação**: nesta etapa é calculado o valor a ser cobrado baseado nas informações obtidas pelo ciclo da classificação. A estrutura tarifária é representada por uma tabela com os custos de cada categoria de serviço. Esta tabela pode ser alterada quando necessário e normalmente estas alterações dependem do provedor dos serviços.

d) **Cobrança**: trata do processo de armazenamento das informações de cobranças e o envio destas cobranças ao consumidor (a entidade a qual o serviço está sendo entregue). O intervalo da cobrança pode ser mensal, diário, por horas ou por um intervalo que depende do acordo negociado entre o consumidor e o provedor de serviços.

3.2 Obstáculos no Contexto de Contabilidade TINA

A contabilidade em TINA é composta por complexas atividades dos objetos distribuídos, a qual uma arquitetura computacional e de engenharia ainda devem ser estudadas para garantir a flexibilidade e a confiabilidade. A seguir serão citados alguns dos problemas já identificados com relação à contabilidade TINA (HAMADA, 1996).

- **Contabilidade como parte do serviço de gerenciamento FCAPS**: refere-se às estruturas computacionais e de engenharia necessárias para a solução de problemas em nível de recursos do serviço de gerenciamento FCAPS. Por exemplo, contabilidade (em particular medição) e segurança (em particular a auditoria) compartilham interesses comuns nas atividades de um objeto.
- **Contabilidade distribuída**: refere-se ao fato de que as entidades de contabilidade em TINA como o gerenciador de medição, cobrança, etc. são distribuídos, assim como os objetos da contabilidade. Um recurso pode ser compartilhado entre diferentes serviços e diferentes gerenciadores de medição. Neste contexto de gerenciamento distribuído, também é considerado como se pode garantir que as informações de eventos são transformadas em informações da medição consistentes. Esta natureza distribuída ainda impõe outros problemas como por exemplo, a medição é possivelmente executada pelo Servidor de Notificações do DPE ou pelo mecanismo de *EventReport/Notification* (ITU, 1993) do TMN, ou por algum outro mecanismo correspondente. Neste caso, informações de eventos não possuem garantia de que serão entregues, ou estas informações poderão se perder e as informações da medição resultante não serão completos.
- **Aspectos dinâmicos da contabilidade**: refere-se à situação em que as estruturas tarifárias e categorias de classificação estão sujeitas às alterações

devido às mudanças das necessidades do mercado e ao desenvolvimento de novos serviços e a remoção de serviços existentes. Também pode ser dito que o ciclo da medição é dependente do serviço e da sua estrutura tarifária correspondente.

- **Associação de funções flexíveis na contabilidade**: tradicionalmente existe uma diferença entre quem é o fornecedor de serviço e quem é o usuário. Este conceito deve ser reexaminado e redefinido para que suporte o conceito cliente-servidor distribuído de TINA. Por exemplo, no conceito em camadas TINA, um provedor de serviço pode ser um usuário (cliente) de outro provedor de serviço.

3.3 Arquitetura de Contabilidade Básica

Os problemas da contabilidade em TINA são associados aos conceitos do Contexto de Gerenciamento de Contabilidade (*AcctMgmtCtxt – Accounting Management Context*) e da Transação de Serviço. O propósito do *AcctMgmtCtxt* é de garantir que a contabilidade seja preservada através das atividades de um conjunto de objetos distribuídos, as quais constituem um serviço. É necessário enfatizar que a contabilidade não é uma propriedade ou um atributo de um simples objeto, mas sim um conjunto de grandezas medidas (ou calculadas) sobre as atividades dos objetos distribuídos durante o serviço (HAMADA, 1996).

Na Figura 3-2 é ilustrado o modelo de informações da Transação de Serviço e do Contexto de Gerenciamento de Contabilidade. Cada componente do Contexto de Gerenciamento de Serviço FCAPS especifica os detalhes da qualidade e quantidade dos serviços de gerenciamento. O Contexto de Gerenciamento de Contabilidade particularmente especifica os 5Ws (o que, como, quando, quem e onde – *What, hoW, When, Who, Where*) da Gerência de Contabilidade. Quando uma Transação de Serviço é ativada pelo SSM (*Service Session Manager*), seu *AcctMgmtCtxt* é interpretado de acordo com sua Descrição de Componente de Sessão (unidade de serviço a ser contabilizado) e com a estrutura de tarifa dentro do domínio SSM. O SSM repassa o controle e os parâmetros necessários para os mecanismos em nível dos recursos

computacionais tais como CSM (*Communication Session Manager*), *Notification Server* e gerenciadores de medição.

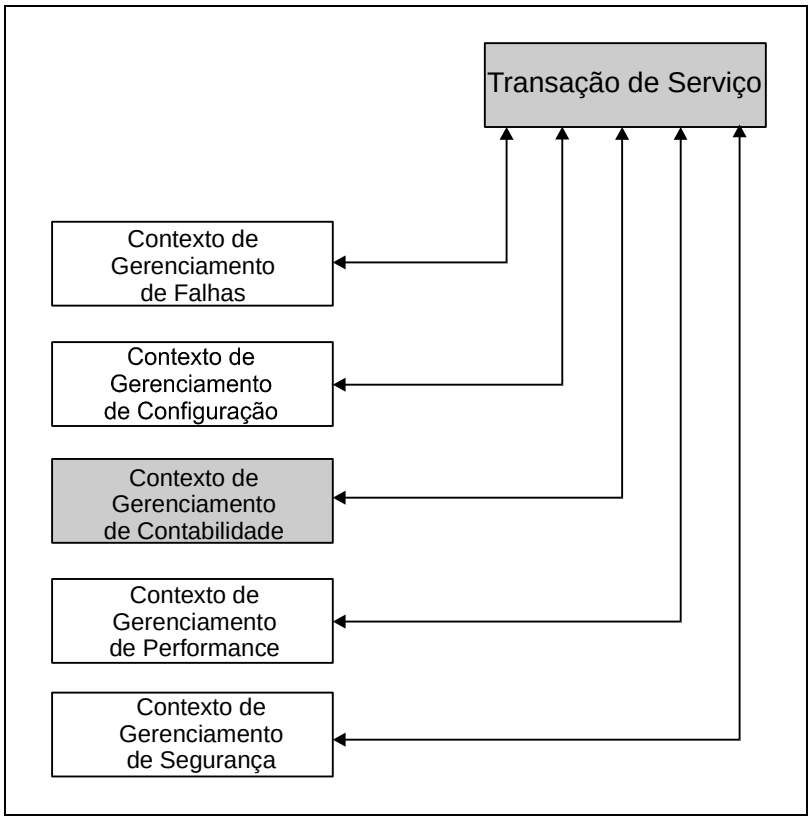

Figura 3-2 Transação de Serviço e o Contexto de Gerenciamento FCAPS.

A associação dos conceitos de Transação de Serviço e do *AcctMgmtCtxt* possui as seguintes conseqüências no processo de contabilidade TINA:

- **Contabilidade garantida**: a Transação de Serviço deve oferecer mecanismos que garantam a integridade do serviço.

- **Controle do processo de contabilidade flexível**: implica que o processo de contabilidade pode ser facilmente adaptado aos diferentes domínios através de mecanismos adequados de interpretação. Como a interpretação do *AcctMgmtCtxt* adiciona um maior nível de flexibilidade, pode-se dizer que o processo é facilmente adequado às mudanças nas estruturas tarifárias ou no ambiente do serviço.

- **Contabilidade eficiente**: os parâmetros de controle da contabilidade em nível dos recursos, como do ciclo *Event Report,* podem ser otimizados na interpretação do *AcctMgmtCtxt* no SSM. Isto é possível devido à estrutura das informações da medição. A freqüência da medição deve ser determinada a partir das especificações do componente de sessão e do ambiente do domínio de serviço.

- **Contabilidade distribuída**: a tarefa da contabilidade pode ser dividida entre processos concorrentes ou dividido entre o usuário e o provedor do serviço. Em TINA, o processo de contabilidade utilizando o *AcctMgmtCtxt* possibilita que, com mecanismos de segurança apropriados, a tarefa da contabilidade seja dividida entre o usuário e o provedor de serviços, transferindo parte da responsabilidade de contabilidade para o usuário.

- **Contabilidade confiável**: as informações da contabilidade devem ser confiáveis. A necessidade da confiabilidade parte da natureza distribuída de TINA. Eventos podem ser perdidos devido aos congestionamentos temporários da rede ou informações da medição podem ser perdidos devido a uma falha no nó. Pode-se esperar que algumas destas questões sejam tratadas pela gerência de falhas, mas a consistência e a confiabilidade das informações de contabilidade devem ser tratadas pela própria gerência de contabilidade.

- **Contabilidade confiante**: as informações de contabilidade devem ser verídicas. Esta necessidade vem da natureza aberta de TINA. Um usuário e um provedor de serviços, totalmente desconhecidos entre si, podem se conectar utilizando algum tipo de catálogo eletrônico (*Yellow page*). Como o usuário pode confiar no provedor de serviços e como o provedor de serviços pode confiar no usuário? A primeira questão está mais relacionada com a gerência de contabilidade, enquanto que a segunda está mais relacionada com a gerência de segurança. Informações de contabilidade devem ser confiáveis e gravadas em ambos os lados (opcionalmente) de uma maneira inalterável e irrefutável.

- **Integridade das informações de contabilidade**: a integridade das informações da contabilidade devem ser preservadas apesar de possíveis falhas na rede,

interrupções de serviços e do encaminhamento do serviço através de diferentes domínios de gerência.

3.4 Transação de serviço (*Service Transaction*)

Nesta seção o conceito de Transação de Serviço é explanado. A Transação de Serviço é composta por três fases muito importantes para executar uma sessão (HAMADA, 1996):

3.4.1 Fase *Setup*

O usuário apresenta seu esquema de contabilidade e o provedor de serviços também apresenta seu esquema de contabilidade (é possível o caso de negociação entre as partes). Quando os dois esquemas fornecidos estiverem compatíveis, um consistente *AcctMgmtCtxt* pode ser formado. O esquema negociado é submetido ao *AcctMgmtCtxt* da sua respectiva Transação de Serviço. O *AcctMgmtCtxt* é interpretado através da leitura das especificações do componente de sessão e do ambiente de contabilidade do domínio. Os mecanismos em nível de recursos são configurados de maneira a seguir as interpretações.

3.4.2 Fase *Execution*

O serviço é oferecido ao usuário de acordo com as especificações da Transação de Serviço. Informações da medição são acumuladas nos respectivos componentes em nível de recursos (registros da conta do usuário, gerenciador da medição, registros da conta do provedor de serviços, etc.), a qual é especificado como parte do *AcctMgmtCtxt*.

3.4.3 Fase *Wrap-up*

O serviço é concluído e as informações da medição em localizações possivelmente distribuídas são coletadas e sumarizadas. Informações de cobrança podem ser enviadas ao usuário na conclusão da transação. A transação é concluída com sucesso se as informações de contabilidade estão de acordo com o *AcctMgmtCtxt*, ou consideradas

incompletas se não estiverem de acordo com o *AcctMgmtCtxt*. Neste último caso, ações corretivas podem ser tomadas.

3.5 Aninhamento de Transações de Serviços

Como um serviço pode ser encaminhado por agentes que não são controlados diretamente pelo usuário ou como um serviço pode se estender sobre diversos Domínios de Gerenciamento, é necessário que ao menos uma parte dos termos de contabilidade do *AcctMgmtCtxt* do usuário sejam encaminhados juntamente com as atividades distribuídas iniciadas pelo usuário. Por exemplo, um usuário pode ativar um serviço encaminhado por um agente (p. ex.*QoS broker*), que por sua vez usa um outro agente para executar certas funções (p. ex. *bandwidth broker*), e assim por diante. Um conjunto de agentes pode ser ativado em cascata, onde o fim da corrente executa alguma função relacionada com o Contexto de Gerenciamento de Serviço inicialmente configurado entre o usuário e o provedor de serviços (HAMADA, 1996).

O propósito do conceito de Transação de Serviço é oferecer um Contexto de Gerenciamento de Serviço consistente através das atividades distribuídas dos objetos. A Figura 3-3 ilustra um serviço estendido por diversos Domínios de Gerência de Serviço.

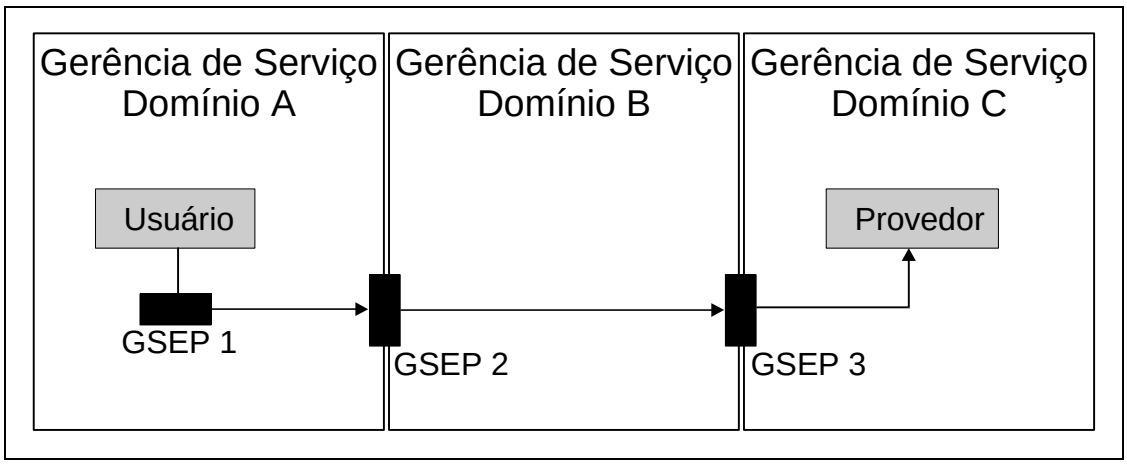

Figura 3-3 Serviço através de múltiplos Domínios de Gerência de Serviço

(HAMADA, 1996).

1. O usuário submete um serviço dentro do domínio “A” através do GSEP1 (*Generic Session End Point*). Com o serviço encaminhado, ele pode

eventualmente ativar um serviço em um domínio diferente (no caso, domínio "B") através do GSEP2. O usuário pode ou não saber da existência de GSEP2 ou de que um serviço do domínio "B" está sendo acessado pelo serviço que ele submeteu.

2. O serviço no Domínio "B" pode ser encaminhado por um SSM, ou pode ser encaminhado por um conjunto de agentes que atuam de maneira relativamente independente. Ele pode eventualmente alcançar GSEP3, que é o ponto de entrada para o Domínio "C".
3. Através do GSEP3, o provedor oferece um serviço. O provedor em si pode ou não estar visível a partir do Domínio "B", da mesma maneira que o provedor também pode ou não estar visível para o usuário.

Utilizando o conceito de aninhamento da Transação de serviço, a Figura 3-3 pode ser reestruturada como ilustra a Figura 3-4.

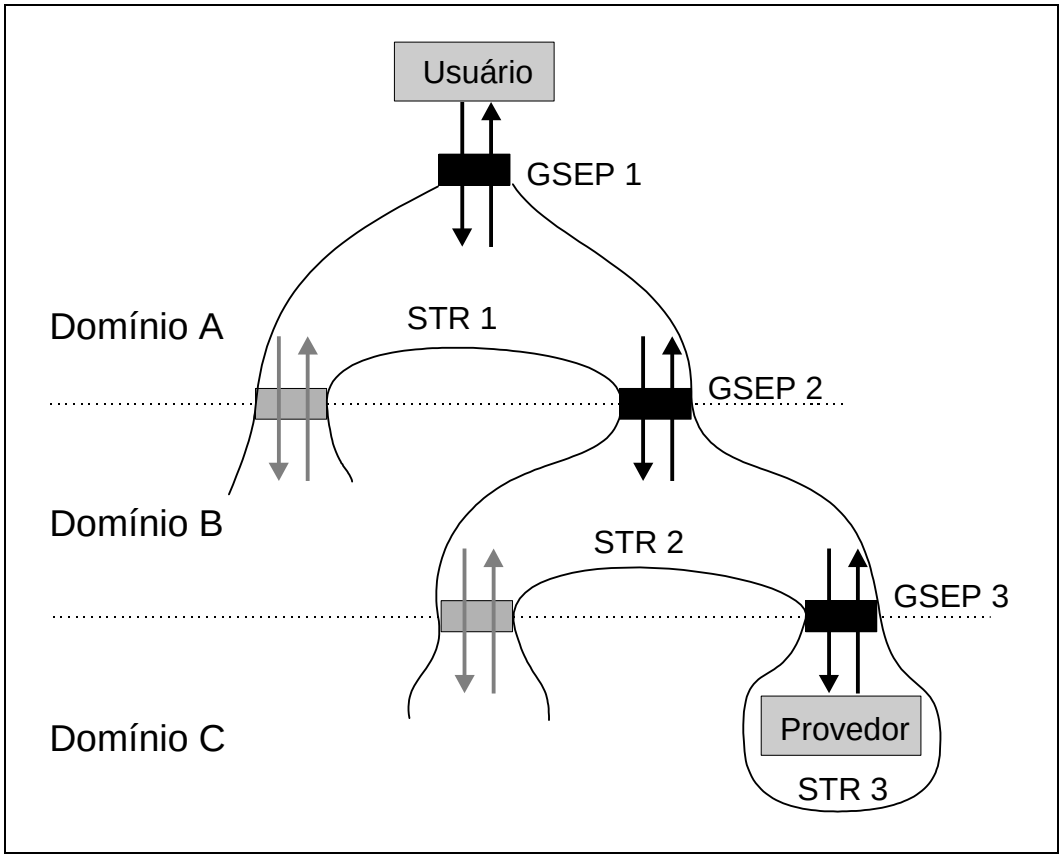

Figura 3-4 Estrutura de aninhamento da Transação de Serviço (HAMADA, 1996).

As curvas sólidas na Figura 3-4 representam os limites do escopo das Transações de Serviço. O escopo da Transação de Serviço geralmente coincide com seu respectivo Domínio de Gerência de Serviço. Uma passagem por domínio diferente (GSEP1, GSEP2) requer uma nova Transação de Serviço para iniciar um ponto de entrada (*entry point*)

O conceito da Resolução de Escopo no Contexto de Gerenciamento de Serviço serve para se determinar a qual contexto a transação aninhada pertence antes que a transação inicie sua execução. Para explanar o problema do escopo, a seguir são dadas algumas propriedades do aninhamento de Transações de Serviço (utilizando a Figura 3-4 como exemplo):

- **A transação raiz (STR1) é concluída somente quando todas as transações aninhadas (STR2, STR3) concluírem suas funções**: isto não quer dizer necessariamente que todas as transações aninhadas devem ser concluídas com sucesso. Por exemplo, se o esquema de *back-up* parcial está aplicado na transação raiz e se algumas das transações aninhadas falhar, o usuário pode ser capaz de utilizar apenas os resultados bem sucedidos e a transação raiz pode ser concluída com sucesso parcial.

- **Se a transação raiz abortar, todas as transações aninhadas devem abortar**: este caso ocorre quando somente uma das transações aninhadas falhar e o esquema de *back-up all abort* é utilizado. Isto quer dizer que quando o *AcctMgmtCtxt* não pode se tornar visível, todo o serviço deve ser abortado.

3.6 Contexto do Gerenciamento da Contabilidade (*AcctMgmtCtxt*)

O *AcctMgmtCtxt* é um bloco de informações e parte fundamental da Contabilidade TINA, a qual especifica o 5W (*What, hoW, When, Who, Where*) do ciclo básico da contabilidade. A Figura 3-5 ilustra o modelo do *AcctMgmtCtxt* (HAMADA, 1996):

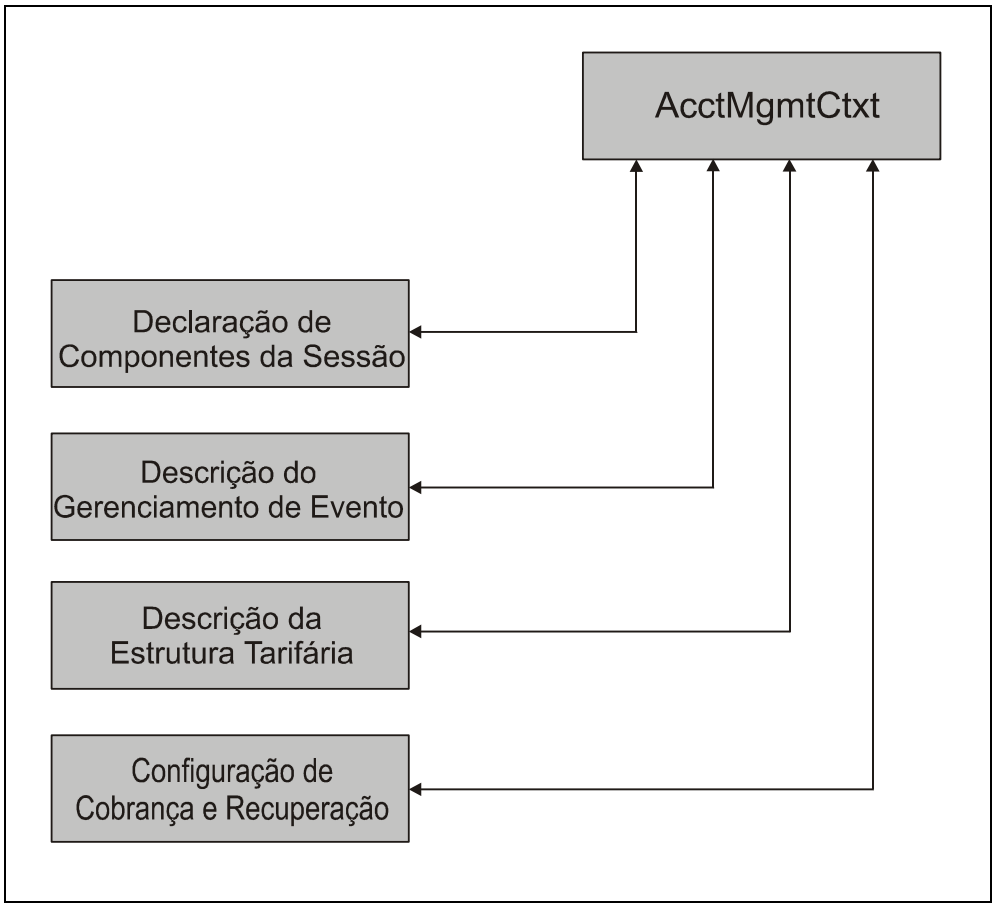

Figura 3-5 Modelo *AcctMgmtCtxt* .

1) Declaração dos Componentes da Sessão

Esta parte define quais Componentes de Sessão serão usados ou se um componente de sessão específico será possivelmente usado na Transação de Serviço especificado pelo *AcctMgmtCtxt*. A função desta parte é declarar quais Componentes de Sessões estão disponíveis ou visíveis ao usuário, como parte distinguível do serviço, possibilitando que o usuário especifique ou negocie o gerenciamento de eventos que será descrito a seguir na Descrição de Gerenciamento de Eventos. A Declaração dos Componentes de Sessão pode ser omitida caso ele já tenha herdado informações da Transação de

Serviços. É preciso que o Componente de Sessão seja uma parte distinguível do serviço, onde tanto o usuário quanto os provedores de serviços sejam capazes de identificar a sua existência e diferenciá-lo de outros componentes. Pode-se citar como exemplo uma típica ligação telefônica a qual consiste das seguintes fases: fase-discar, fase-chamar, fase-falar, fase-desligar, fase-ocupado, etc. Estas fases são partes distintas do serviço e podem ser consideradas como Componentes de Sessão.

2) Gerenciamento de Eventos

Esta parte especifica os 5Ws dos eventos gerados ou associados a cada Componente de Sessão. Por exemplo, no início de cada Componente de Sessão, o usuário pode desejar ser notificado ou o provedor de serviços pode necessitar de uma confirmação do usuário. Diferentes eventos podem ser gerados para cada Componente de Sessão ou agrupados em classes para simplificar as ações entre o usuário e o provedor de serviços. Eventos e configurações pré-definidas são derivados de outras partes do *AcctMgmtCtxt*, possibilitando desta maneira uma contabilidade com especificações pré-definidas sem que as Descrições de Gerenciamento de Eventos seja alterado pelo usuário ou pelo provedor. Os eventos e ações aqui mencionados estão relacionados apenas com a contabilidade, ou seja, não estão relacionados com as atividades da Sessão de Serviço estabelecida entre o usuário e o provedor.

3) Estrutura de Descrição da Tarifa

Esta parte especifica a estrutura tarifária negociada entre o usuário e o provedor. Esta estrutura tarifária adicionada ao *AcctMgmtCtxt* proporciona uma maior flexibilidade na tarifação, permitindo uma tarifação por usuário, por serviço ou por sessão. Se este tipo de flexibilidade não for necessário, a estrutura tarifária pode ser simplesmente herdada do contrato de assinatura (*subscription*) negociado entre o usuário e o provedor ou herdada da estrutura tarifária pré-definida do Domínio de Gerência de Serviço.

4) Cobrança e Configuração de Recuperação

Esta parte especifica os 5Ws do ciclo de cobrança (*billing*) e das opções de recuperação caso a Transação de Serviço não satisfaça os requisitos da contabilidade. Cobrança e recuperação são assuntos diferentes, mas eles estão combinados dentro de um bloco na

especificação do *AcctMgmtCtxt*, pois eles possuem certas similaridades interessantes do ponto de vista do usuário. Por exemplo, a configuração de cobrança especifica “quem” (quem faz a chamada, cobrança de terceiros, cobrança compartilhada, etc.), “quando” (mensal, semanal, cobrança on-line, etc.) no ciclo de cobrança. Como opções de recuperação existem a opção do esquema de *back-up* parcial e o esquema de *back-up all abort*.

3.7 Conclusão

Neste capítulo foi apresentado a Arquitetura do Gerenciamento da Contabilidade TINA baseada na Transação de Serviço e no conceito do Contexto de Gerência de Contabilidade (*AcctMgmtCtxt*). Estes conceitos podem ser aplicados em diversas classes de serviços e aplicações distribuídos TINA, incluindo aquelas em que a sessão de serviço se expande por múltiplos domínios com múltiplos provedores de serviços com um número de usuários que pode alterar dinamicamente.

No capítulo seguinte, questões de segurança em TINA serão apresentadas, seguidas pela apresentação do conceito de segurança multilateral.

4. Segurança na Contabilidade TINA

4.1 O domínio de segurança em TINA

A segurança está envolvida em todas as partes da arquitetura TINA, ela afeta todas as partes e não pode ser tratada isoladamente. Para enfrentar esta complexidade, é necessário estruturar adequadamente os problemas no domínio de segurança de uma maneira adequada. Todos os serviços e recursos estão sujeitos a ataques e invasões (STAAMANN, 1997).

Ataques podem ser o uso ilegítimo de componentes ou a modificação de dados, configurações ou programas. Estes ataques podem ocorrer através de acessos externos ao sistema, aos dados ou aos serviços ou através da alteração das mensagens trocadas entre os componentes. Os invasores podem tanto ser agentes externos como também participantes dentro da própria rede TINA. Os motivos dos invasores podem ser o uso ilegítimo dos serviços, fraude (negócios on-line), fraude de cobrança, observação de consumidores e provedores, ou ataques de negação de serviço (denial of service).

O objetivo de um ataque pode ser alcançado direta ou indiretamente. No caso deste último, o invasor pode instalar um programa *backdoor*[6] durante o seu primeiro ataque bem sucedido, a qual permitirá que ele retorne mais tarde e continue o ataque. Exemplos de *backdoor* são a alteração de programas ou a alteração de direitos de acesso (STAAMANN, 1997).

Cada participante em uma rede TINA possui o seu próprio Domínio Administrativo. O Domínio Administrativo é um domínio confiável do participante, considerando o fato de que normalmente possui sua própria estrutura física (hardware) e que o software é instalado pelo próprio participante. Este domínio confiável pode ser composto de vários

[6] *Backdoor*- Um programa ou falha existente no sistema que disponibiliza meios de acesso ao sistema. Um programa do tipo “Cavalo de Tróia” pode ser usado para se instalar um *backdoor* no sistema alvo.

nós sobre o controle físico de um participante que são interconectados fisicamente por links inseguros. Estes links podem ser transformados em canais seguros através do uso de criptografia simétrica sem um gerenciamento sofisticado de chaves. Dentro de seu domínio, o participante confia no correto funcionamento do software instalado.

Para interagir com outros domínios (interações interdomínios), relacionamentos confiáveis devem ser estabelecidos. O canal de comunicação entre os domínios não pode ser assumido como seguro, tornando necessária a adição de segurança através de meios criptografados. Todas as partes da arquitetura TINA que estão envolvidas nas interações entre domínios devem possuir segurança, caso contrário um componente sem segurança pode comprometer a segurança de todo o conjunto (STAAMAN, 1997).

4.1.1. Segurança do Sistema

A segurança do sistema deve assegurar que o sistema, principalmente o hardware e o sistema operacional, não estejam sujeitos a invasões. Estão envolvidos os recursos de rede (*switches,* roteadores) e recursos computacionais (Ambiente Nativo de Computação e Comunicação - NCCE, Sistema Operacional e Portas de Comunicação), uma vez que invasões podem não ocorrer nas portas comumente usadas pelo DPE, mas sim em outras portas do NCCE. Por último é considerada a segurança do domínio do usuário final (consumidor), onde os CPEs (*Costumer Premises Equipment*) como computadores pessoais (PCs) ou *workstations,* não se pode assumir que sejam de uso exclusivo como ponto-final de redes TINA.

4.1.2. Segurança do Serviço

A segurança do serviço preocupa-se principalmente em preservar a integridade do controle do serviço. O controle do serviço inclui entre outras atividades a verificação de qual usuário possui permissão para usar um determinado serviço (assinatura) e a contabilidade com finalidade de cobrança. Ambos confiam na identidade autenticada do usuário, ou seja, esta autenticação deve ser suportada por um protocolo para a autenticação do usuário. Usuários anônimos de um serviço pago podem ser autenticados utilizando identidades anônimas (por exemplo, serviço pré-pago). O protocolo de

autenticação deve garantir que informações secretas não possam ser reveladas ou interceptadas por indivíduos não-autorizados. A integridade do controle de serviço inclui a integridade da verificação da assinatura e da contabilidade.

Acessos às funcionalidades dos serviços são controlados em dois níveis, no nível DPE e no nível de serviço. No nível DPE, um simples controle de acesso baseado nas identidades autenticadas dos usuários envolvidos na sessão. No nível de serviço, a lógica de serviço implementada no componente de serviço controla o acesso às informações específicas de serviços e o acesso às funcionalidades baseadas em identidades autenticadas, contextos e informações de estado. A integridade e confidencialidade das informações trocadas entre as interfaces operacionais dos componentes de serviço são conseguidas através da ativação de características apropriadas dos serviços seguros do DPE. Estas características de segurança do DPE devem fornecer não somente a proteção e a integridade das mensagens e sua ordem temporal, mas também a proteção contra interrupções do próprio controle da conexão.

Casos especiais de serviços são os serviços de gerência e os serviços de segurança. Ambos requerem um alto nível de segurança (poderosos mecanismos de autenticação, chaves criptográficas longas ou nós fisicamente seguros para sua implementação). Os serviços de segurança especializados fornecem características de segurança especializadas como o suporte para dinheiro digital (*digital cash*), que não está presente em todos os nós DPE, mas que são suportados por provedores dedicados (*retailers* ou provedores terceirizados) no nível de serviço. Os serviços de gerenciamento estão relacionados com a gerência do sistema, serviços e do DPE. A segurança dos serviços de gerência é crucial, uma vez que acessos ilegais às funcionalidades de gerência podem ser usados para a implantação de *backdoors*.

4.1.3. Segurança do DPE

A segurança do DPE é principalmente relacionada com a prevenção de acessos ilegais aos objetos computacionais (CO) e aos grupos de objetos computacionais. As mensagens contendo argumentos, resultados, exceções, invocações de objetos e notificações também são protegidas. Os nós DPE também devem fornecer meios para

auditorar e reportar eventos de segurança relevantes que ocorreram no nó de acordo com especificações de auditoria definidas pelo administrador. A segurança do DPE inclui a segurança das implementações do DPE e de seus serviços básicos, como o Serviço de Objetos CORBA.

4.1.4. Segurança do conteúdo da comunicação

A segurança do conteúdo da comunicação está relacionada com a autenticação, integridade e confidencialidade das informações do serviço de conteúdo. Como todas as informações do serviço de conteúdo é enviado sob a forma de fluxo (*stream*), este tipo de segurança é adequada somente para fluxos. Fluxos são protegidos através de mecanismos de criptografia, preferencialmente por cifras ou outros tipos especiais de cifras para certos formatos de informações como voz e/ou vídeo. Se o serviço implementado pelo domínio do provedor não requerer nenhuma modificação do fluxo entre os dois pontos, então se pode estabelecer uma segurança ponto a ponto. Caso contrário somente a segurança no lado do provedor pode ser estabelecida. O controle de serviço se encarrega da gerência das chaves necessárias.

Para garantir estes conceitos de segurança em TINA definidos nos 4 itens anteriores é que se pretende implementar uma estratégia e políticas de segurança utilizando os conceitos de segurança multilateral.

4.2 Segurança Multilateral

A segurança multilateral tem por objetivo fornecer segurança para todos os participantes envolvidos, requerendo de cada participante um mínimo de confiança na honestidade dos outros participantes envolvidos (PFITZMANN, 2002):

- Cada participante tem seus **objetivos de proteção** particulares.
- Cada participante pode formular seus objetivos de proteção.
- Conflitos de segurança são reconhecidos e os compromissos negociados.
- Cada participante pode reforçar seus objetivos de proteção dentro do compromisso negociado.

A segurança multilateral não possibilita necessariamente que todos os participantes possam reforçar ser objetivos de segurança individuais, mas ao menos ela provê a transparência de todas as ações relacionadas à segurança de todos os participantes envolvidos.

4.2.1 Objetivos de Proteção, suas sinergias e interferências.

Em discussões ocorridas principalmente nas esferas governamentais nos últimos 17 anos, a confidencialidade, a integridade, a disponibilidade e a contabilidade foram definidas como intimamente relacionadas com a segurança de um sistema. Fora da esfera governamental, os conceitos de anonimato (*anonymity*) e da não-observabilidade também se tornaram grandes ítens relacionados à segurança, decorrente do avanço das tecnologias de armazenagem que tornou possível o registro permanente de informações pessoais por um custo muito baixo (PFITZMANN, 2001).

Para uma melhor compreensão dos objetivos de segurança no contexto de comunicação em redes de computadores, na Tabela 4-1 é dada a diferença entre conteúdo e circunstâncias da comunicação.

PROTEÇÃO / AMEAÇA	Conteúdo	Circunstâncias
Acesso não autorizado à informação	Confidencialidade Ocultação	Anonimato Não observalidade
Modificação não autorizada da informação	Integridade	Contabilidade
Alteração não autorizada das funcionalidades	Disponiblidade	Alcançabilidade

Tabela 4-1: Objetivos de Proteção (PFITZMANN, 2001)

Existem algumas sinergias e interferências entre os objetivos de segurança, de modo que o relacionamento entre certos objetivos de segurança pode ocasionar dificuldades para um (ou ambos) objetivo(s) de segurança. Também ocorrem casos onde o relacionamento entre dois objetivos de segurança termina por fortalecer um (ou ambos) objetivo(s) de segurança. Essa relação é apresentada na Figura 4-1

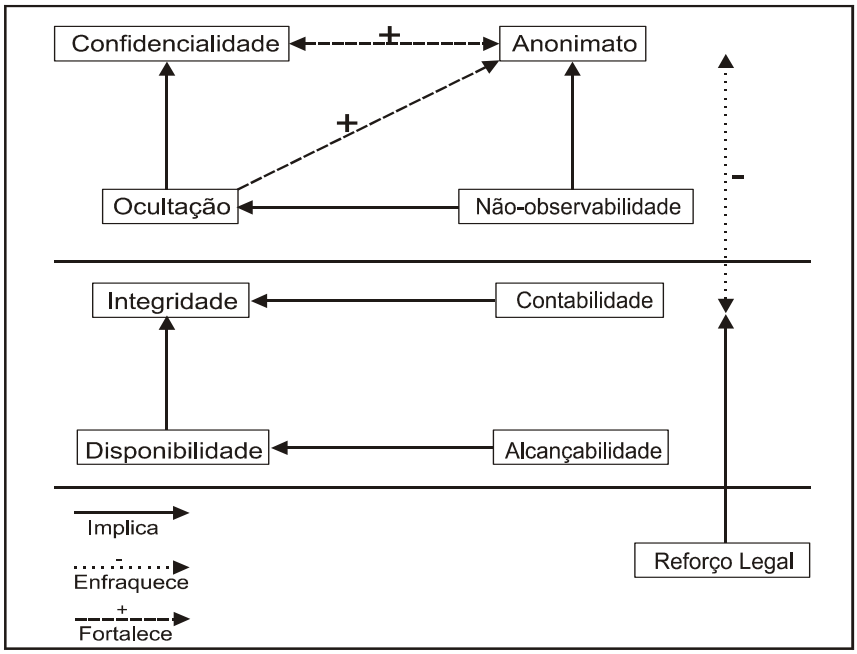

Figura 4-1: Sinergias e interferências entre objetivos de proteção (PFITZMANN, 2001)

Pftizmann em (PFITZMANN, 2001) introduz a classificação de tecnologias para a segurança multilateral de acordo com o número de participantes em um dado momento e também descreve as distinções entre tecnologias unilaterais, bilaterais, trilaterais e multilaterais.

a) Tecnologias Unilaterais

Tecnologias unilaterais são tecnologias onde cada participante pode decidir por si próprio as regras de segurança. Assim, a coordenação e a negociação não são necessárias para o seu uso. Tecnologias unilaterais importantes para a segurança multilateral são:

- Ferramentas para ajudar usuários inexperientes a definirem seus objetivos de segurança. Se necessário, para cada aplicação ou até mesmo para cada ação.
- Dispositivos (portáveis ou não) as quais são seguros para seus usuários de maneira a incrementar a segurança. Esses dispositivos devem prover pelo menos **proteção física** para a entrada/saída de dados com seus usuários e, se esse dispositivo possuir mais de uma utilidade, ele deve utilizar um sistema operacional que ofereça controle e administração detalhados dos direitos para

aplicações, aderindo ao princípio do **mínimo privilégio**[7]**.** Isto é essencial para limitar a disseminação de programas maliciosos como os vírus de computador.

- Criptografia da mídia local de armazenamento e/ou autenticação de seu conteúdo, veja Figura 4-2.
- Ocultar dados secretos no conteúdo multimídia local ou no sistema de arquivos, não somente para esconder o conteúdo dos dados secretos, mas também a sua própria existência. Essa ocultação pode ser alcançada através do emprego de técnicas esteganográficas[8] (ANDERSON, 1998).
- Adição de *"marcas d´agua"* ou *"impressão digital"* aos dados usando técnicas esteganográficas para auxiliar na identificação de violações de autoria e direitos autorais.
- Usando somente softwares os quais o código-fonte seja aberto e amplamente checado ou que possua segurança certificada por terceiros. Estes terceiros devem possuir acesso completo ao seu código fonte e às ferramentas utilizadas para a geração do código. A melhor técnica é combinar ambas as abordagens de maneira a avaliar o mais profundo possível o software. Isto é possível usando ao menos uma destas duas abordagens para que se tenha uma certeza razoável se o software utilizado não possua "Cavalos de Tróia". Uma avaliação semelhante deve ser aplicada ao hardware onde todas as ferramentas usadas para o desenvolvimento e produção sejam checadas para se verificar a ausência de programas do tipo "Cavalo de Tróia".

---

[7] **Princípio do mínimo privilégio**: o usuário (ou uma aplicação) não precisa ter mais autoridade do que o mínimo necessário para que executem adequadamente suas funções.

[8] Esteganografia: escrita em cifras em caracteres convencionais ou especiais.

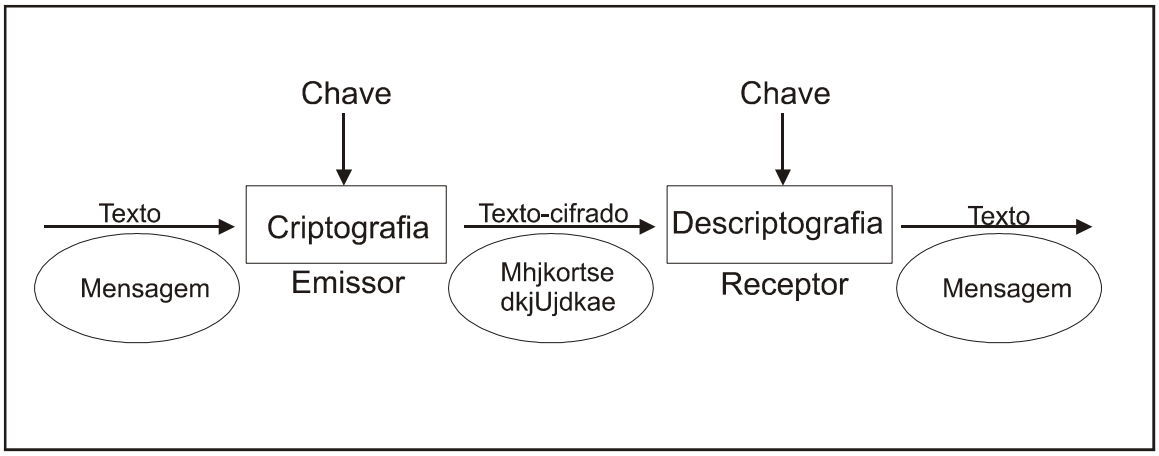

Figura 4-2: Processo de criptografia e descriptografia de uma mensagem.

b) Tecnologias Bilaterais

Tecnologias Bilaterais podem ser utilizadas somente quando ambos os participantes cooperam. Isto significa que ao menos alguma coordenação e negociação é necessária para que seu uso possa ser efetivo.

Tecnologias bilaterais importantes para a segurança multilateral são:

- Ferramentas para negociar objetivos de proteção bilaterais e mecanismos de segurança.
- Mecanismos de criptografia e mecanismos de esteganografia para assegurar o conteúdo da comunicação.

c) Tecnologias Trilaterais

Tecnologias trilaterais somente podem ser usadas se um terceiro participante é envolvido de maneira a executar uma determinada tarefa para outros participantes. Isto significa que mais coordenação e negociações são necessárias em comparação às tecnologias unilaterais e bilaterais. Tecnologias trilaterais importantes para segurança multilateral são:

- Ferramentas para negociar mecanismos trilaterais de segurança, por ex. para contabilidade.
- Uma infraestrutura de chave pública (PKI), para fornecer aos usuários chaves públicas certificadas de outros usuários para conferir suas respectivas assinaturas digitais e para dar aos usuários a habilidade de revogar sua própria chave pública se a chave privada correspondente se tornar comprometida.

- *Gateways* de segurança para “traduzir” incompatibilidades ou detalhes entre mecanismos de segurança. Os *gateways* de segurança funcionam bem em mecanismos de integridade e contabilidade, mas são questionáveis para mecanismos de confidencialidade e anonimato. Os *gateways* de segurança não podem “traduzir” incompatibilidades entre objetivos de proteção.
- Mecanismos que forneçam pseudônimos digitais, isto é, uma combinação adequada de anonimato com contabilidade. Em particular, existem mecanismos que tornam segura a transferência de assinaturas entre diferentes pseudônimos de um mesmo participante.

Quando pseudônimos são usados durante a troca de informações de contabilidade, existe uma quantidade de possíveis tarefas para terceiros integrados, tais como:

- Identificação do usuário em um evento de fraude (pseudônimos são certificados e a autoridade certificadora conhece sua identidade real), isto é, a privacidade de pseudônimos não pode ser garantida.
- Depósito obrigatório de pagamento de um “fiador” para prevenir fraude em virtude da completo anonimato dos pseudônimos, isto é, privacidade dos pseudônimos pode ser garantida.

d) Tecnologias Multilaterais

Tecnologias multilaterais somente podem ser usadas se um grande número de participantes independentes cooperarem. Isto significa que coordenação e negociação são necessárias em larga escala. Tecnologias multilaterais importantes para a segurança multilateral são:

- Ferramentas para negociar objetivos de proteção multilaterais e mecanismos de segurança, como por exemplo, para o anonimato e não-observalidade.
- Mecanismos para prover anonimato, não-observalidade e *unlinkability.*
- Comunicações: proteger quem comunica, quando, para quem e para onde.
- Pagamentos: proteger quem paga e quem recebe.
- Troca de valores: proteger transações eletrônicas de observadores.

4.3 Trabalhos correlatos em segurança multilateral

Atualmente pode-se observar diversos trabalhos referentes ao conceito de segurança multilateral, cujos principais conceitos podem são descritos em (RANNEMBERG, 2000), em (PFITZMANN, 2001) e em (PFITZMANN,2002). Em (SAILER, 1999) é demonstrado como identificar problemas de segurança e assim, aplicar medidas de segurança adequadas.

A segurança multilateral se baseia no uso integrado de diversas outras tecnologias e abordagens, como em (CLAUβ, 2001) que trata da gerência de identidades, em (ANDERSON, 1998) que demonstra o uso de mecanismos esteganográficos para ocultar informações e em (BLEUMER, 2000) que introduz o uso da autenticação biométrica, que fornece um alto nível de segurança por estar relacionado com um perfil físico-biológico único de cada indivíduo.

A aplicação da segurança multilateral em redes de telecomunicações é discutida em (BUTTÝAN,1999) com ênfase em arquiteturas que utilizem como base um DPE, como a arquitetura TINA, por exemplo. Em (SAILER, 1998) é descrita uma abordagem para prover serviços seguros em redes de telecomunicações ISDN/IN.

Para validar os conceitos da segurança multilateral, em (PFITZMANN, 1998) um sistema de aplicação distribuída foi implementado usando-se o Java como linguagem para a programação e o Java RMI (*Remote Method Invocation*) para dar suporte ao ambiente distribuído. (RANNENBERG, 2000) também apresenta um protótipo baseado em PDA´s (Portable Digital Assistance) Newton[9] a telefones celulares GSM.

4.4 Conclusão

Neste capítulo foram apresentados as possíveis vulnerabilidades que um sistema TINA está sujeito e os principais requisitos de segurança para cada tipo de serviço oferecido por um sistema TINA. Na seqüência, foram introduzidos os conceitos da segurança multilateral, os principais tipos de objetivos de segurança e uma breve classificação dos tipos de segurança multilateral segundo (PFITZMANN, 2000). Por fim, alguns dos principais trabalhos correlatos em segurança multilateral são listados.

---

[9] Dispositivo portátil desenvolvido pela Apple Computer.

5. Um Modelo de Segurança no Gerenciamento de Contabilidade TINA

Utilizando como base os conceitos e definições apresentados nos três capítulos anteriores, neste capítulo será apresentada a proposta para o modelo de segurança no gerenciamento de contabilidade baseado na arquitetura TINA.

O conceito da segurança multilateral se ajusta bem ao ambiente para a qual a arquitetura TINA foi idealizada. Em uma sessão TINA ocorre a interação entre diversos participantes que podem ser totalmente desconhecidos entre si, mas que precisam de um mínimo de segurança para que o serviço seja oferecido com sucesso. Para que a segurança da contabilidade seja alcançada, é necessário prover segurança para todas as interações que ocorram entre os participantes.

A Figura 6-1 ilustra uma situação onde os Usuários A e B acessam um serviço de videoconferência oferecido pelo Provedor. O Intermediário é quem fornece a localização do provedor para usuário, como também a localização do Provedor de Serviços Terceiros para o Provedor. O Provedor de Conectividade é o responsável pelo transporte das informações de controle e do conteúdo contratado pelo usuário ou pelo provedor.

Cada ligação entre os participantes na Figura 5-1 representa uma sessão de comunicação que deverá se estabelecer entre os participantes.

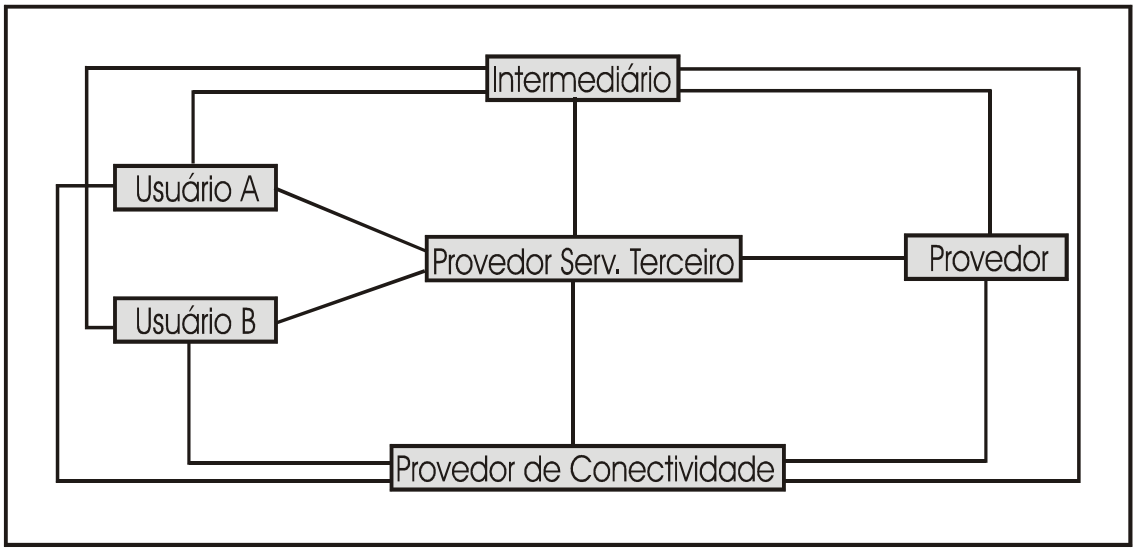

Figura 5-1: Exemplo de uma sessão TINA.

5.1 Proposição do Modelo

Neste modelo será criado o conceito do Contexto de Gerenciamento de Segurança (*SecMgmtCtxt*) que irá permitir a coordenação de todo o comportamento da Transação de Serviço com relação aos interesses de segurança definidos para um determinado *SecMgmtCtxt*. A estrutura do *SecMgmtCtxt* é muito semelhante ao do *AcctMgmtCtxt*, tendo o mesmo domínio e tempo de vida. A estrutura do *SecMgmtCtxt* é constituída pelos seguintes componentes:

- **Declaração dos Componentes de Sessão**: A função desta parte é declarar quais Componentes de Sessões estão disponíveis ao usuário, quais são os componentes que já possuem uma relação segura e o nível de segurança que foi estabelecido com um determinado componente.
- **Objetivos de Segurança/ Mecanismos de Segurança**: Discrimina quais objetivos de segurança o participante negociou. Também descreve quais mecanismos de segurança foram adotados para se efetivar os objetivos de segurança desejados.
- **Controle de *Logs***: Registra informações de eventos que ocorram durante a existência do SecMgmtCtxt para fins de auditoria . Estas informações podem ser o tipo de acesso que foi associado a um determinado objeto, quem acessou o objeto ou quem modificou o objeto. Quanto mais detalhado for o tipo de *Log* menor será o desempenho do sistema.

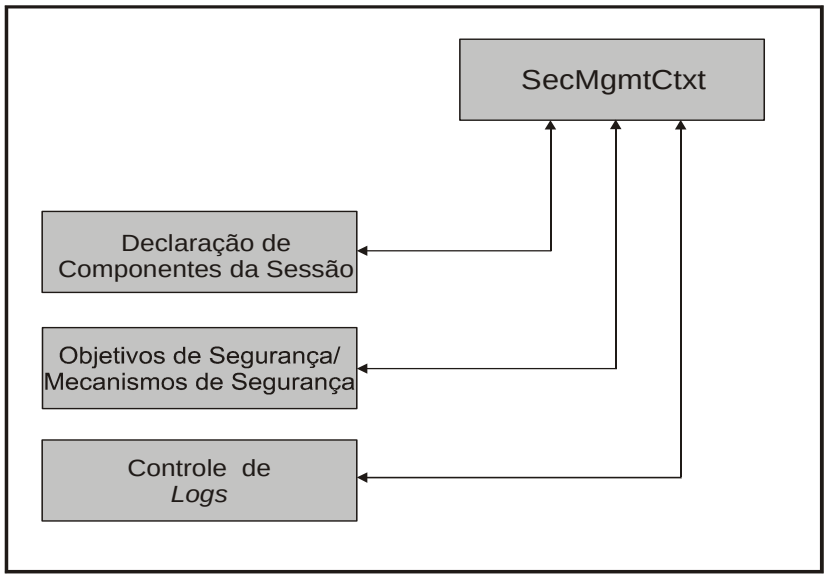

Figura 5-2: Modelo do SecMgmtCtxt

Estes interesses de segurança serão previamente definidos entre os participantes. Como a segurança multilateral possibilita a negociação dos interesses de segurança, ao menos os limites mínimos de segurança dos participantes devem estar definidos antes mesmo de qualquer negociação.

Quando for necessário o estabelecimento de uma sessão de comunicação entre dois participantes (entre um consumidor e um *Retailer*, por exemplo) é verificado se ambos os participantes pertencem ao mesmo Domínio de Gerência. Se eles pertencerem ao mesmo domínio, a sessão é estabelecida normalmente. Caso contrário os participantes fazem parte de Domínios de Gerência distintos e, conseqüentemente, de Domínios de Segurança distintos. Neste último caso, a negociação dos objetivos de segurança é necessária. O Agente de Segurança (SA) será o responsável por esta negociação que pode terminar com sucesso e a sessão de comunicação estabelecida ou por um erro, caso não seja possível negociar um conjunto mínimo de objetivos de segurança.

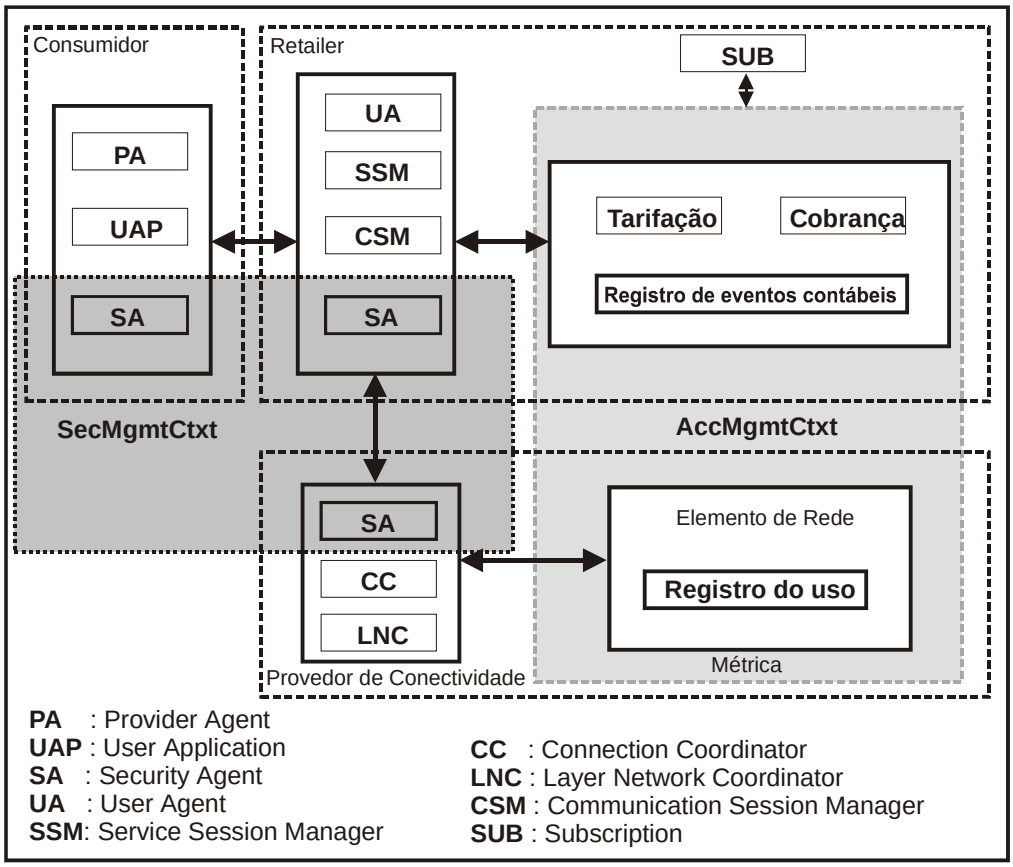

Figura 5-3: Modelo Arquitetural do SecMgmtCtxt e do AcctMgmtCtxt.

5.2 Implementação do protótipo

Alguns dos principais itens necessários para a segurança multilateral que deverão ser adicionados ao protótipo:

- Configuração externa ao usuário das características de segurança das aplicações para expressar suas preferências de segurança,
- Negociação entre os sistemas dos participantes para acertar o problema de diferentes configurações,
- Uma visão abstrata dos mecanismos de segurança assim como uma API abstrata para prover a flexibilidade necessária para a configuração externa.

Configuração: A configuração é a principal parte visível da plataforma para o usuário final. Uma atenção especial deve ser dada aos usuários com pouca experiência.

Interface ao usuário: A interface ao usuário habilita ao usuário final a fácil configuração de mecanismos de segurança e serviços para o seu sistema e suas aplicações distribuídas. A interface de configuração de segurança do sistema é parte do SA e provê a possibilidade de “entrar” dados de configuração centrais as quais formarão a base para a configuração da segurança pra toda a aplicação distribuída.
Para cada objetivo (requisito) de segurança como a confidencialidade, integridade, anonimato ou contabilidade, o usuário pode escolher o mecanismo de segurança de sua preferência. O sistema provê uma lista de mecanismos disponíveis. Novos mecanismos de segurança podem ser adicionados ao sistema posteriormente.
O usuário precisa se decidir sobre qual objetivo de segurança ele deseja alcançar para a sua aplicação.

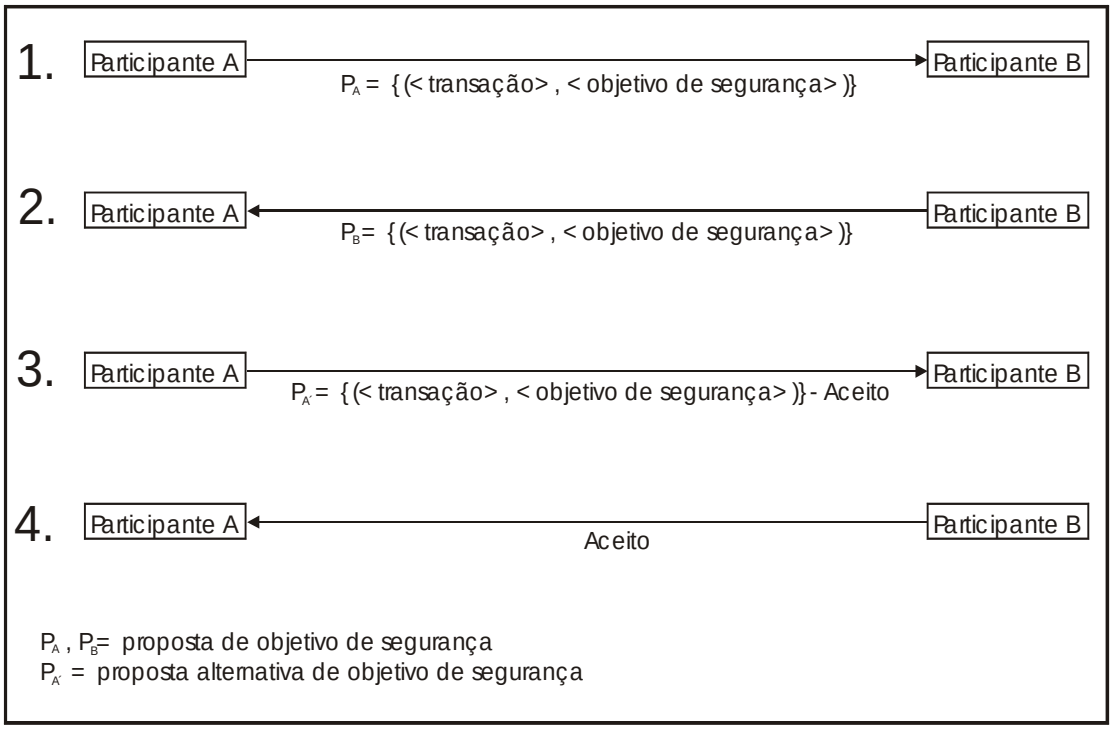

Figura 5-4: Protocolo de Negociação da fase 1.

Negociação. Todos os participantes em uma aplicação distribuída podem configurar seus respectivos sistemas de acordo com os seus objetivos de segurança. Naturalmente, diferenças na configuração irão surgir. A melhor maneira para sobrepor estas diferenças é a negociação entre as partes envolvidas. De maneira a envolver o usuário o mínimo necessário nas interações, a negociação deve trabalhar o mais automático possível.

A negociação em si de divide em duas partes. Primeiro, os participantes concordam com um objetivo de segurança geral, como confidencialidade ou contabilidade. Depois, os mecanismos utilizados para se atingir este objetivo de segurança são negociados.

Na Figura 5-4, o protocolo desenvolvido para a fase 1 é ilustrado. Ele basicamente mostra que ambos os participantes criam uma proposta para uma possível configuração de segurança em comum. Estas propostas são trocadas e avaliadas. O iniciador da comunicação cria uma proposta que incorpora as propostas de todos os participantes. Se o sistema não for capaz de gerar esta proposta, o componente de negociação informa ao usuário que não foi possível se chegar a um denominador comum para uma comunicação segura. Como resultado, ao menos um dos usuários devem mudar sua configuração de segurança ou a comunicação não poderá ser estabelecida.

Na fase 2, agora com os requisitos de segurança gerais alcançados, o sistema negocia os algoritmos de cifragem. O princípio é o mesmo como descrito acima, mas a solução para conflitos mais sérios se estende para a possibilidade da carga de novos mecanismos do servidor ou a incorporação de um *gateway* de segurança que poderá executar as transformações necessárias entre diferentes mecanismos de segurança.

5.3 Conclusão

Neste Capítulo foi apresentado o modelo proposto como finalidade deste trabalho, em especial o protocolo para se chegar a um consenso através de uma negociação entre os participantes. A estrutura *SecMgmtCtxt* permitirá a coordenação de todo o comportamento da Transação de Serviço com relação aos interesses de segurança definidos pelo participante. Agora que se tem todo o conceito definido, no capítulo seguinte serão observados o resultados obtidos.

6. Resultados da Implementação

Esta implementação fornece a base para a simulação de uma vídeo-conferência entre diversos usuários. Ela é composta por um módulo servidor e um módulo cliente. O módulo servidor é responsável pelo controle dos usuários e por prover o serviço de vídeo-conferência para estes usuários, que por sua vez, utilizam o módulo cliente para interagir na vídeo-conferência. Diversos usuários podem se conectar ao servidor simultaneamente.

Devido a alta complexidade necessária para a implementação de todo o conceito da segurança multilateral na arquitetura de contabilidade TINA, decidiu-se em limitar o escopo da implementação do protótipo na negociação dos objetivos de segurança e na simulação da vídeo conferência com toda a estrutura de contabilidade.

O protótipo foi programado em Java e utiliza a implementação CORBA do Visibroker (VISIBROKER, 1998).

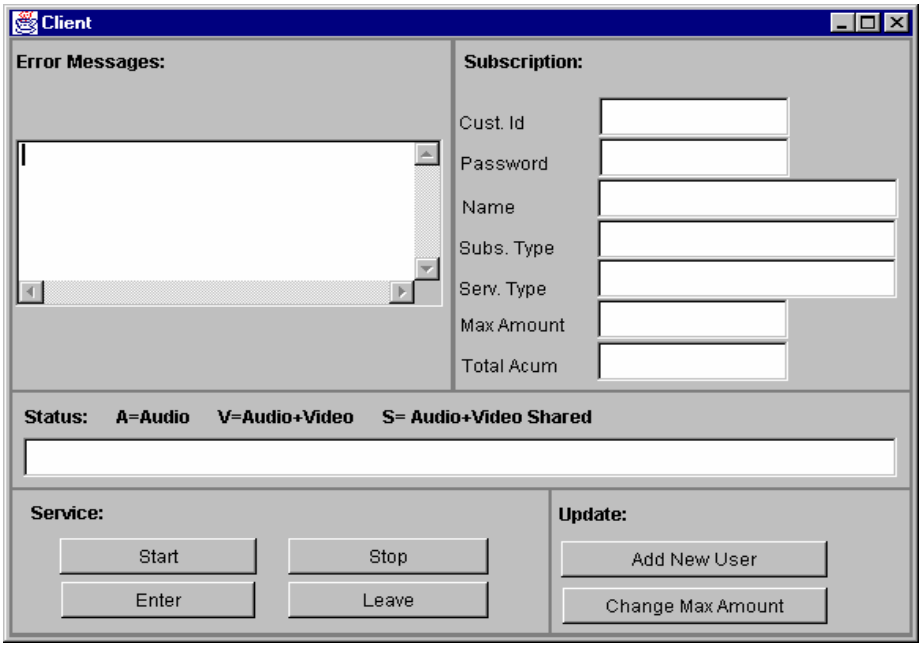

Figura 6-1: Interface Gráfica do Módulo Usuário

A Figura 6-2 apresenta a combinação do modelo de negócios com o modelo computacional baseado nas especificações TINA. Pode-se observar a interação entre

quatro tipos de participantes (Consumidor, Retailer, Provedor de Conectividade e o Provedor) e as estruturas necessárias em cada participante. Essa interação se dá através dos relacionamentos descritos no item 2.2.7.

6.1 Arquitetura de contabilidade

A Figura 5-3 mostra o modelo arquitetural do contexto de gerenciamento de contabilidade (AccMgmtCtxt) com as interações entre os principais componentes da arquitetura de serviço TINA

O *AcctMgmtCtxt* é composto por componentes que abrangem diferentes aspectos do serviço, do controle de rede e do gerenciamento, a saber:

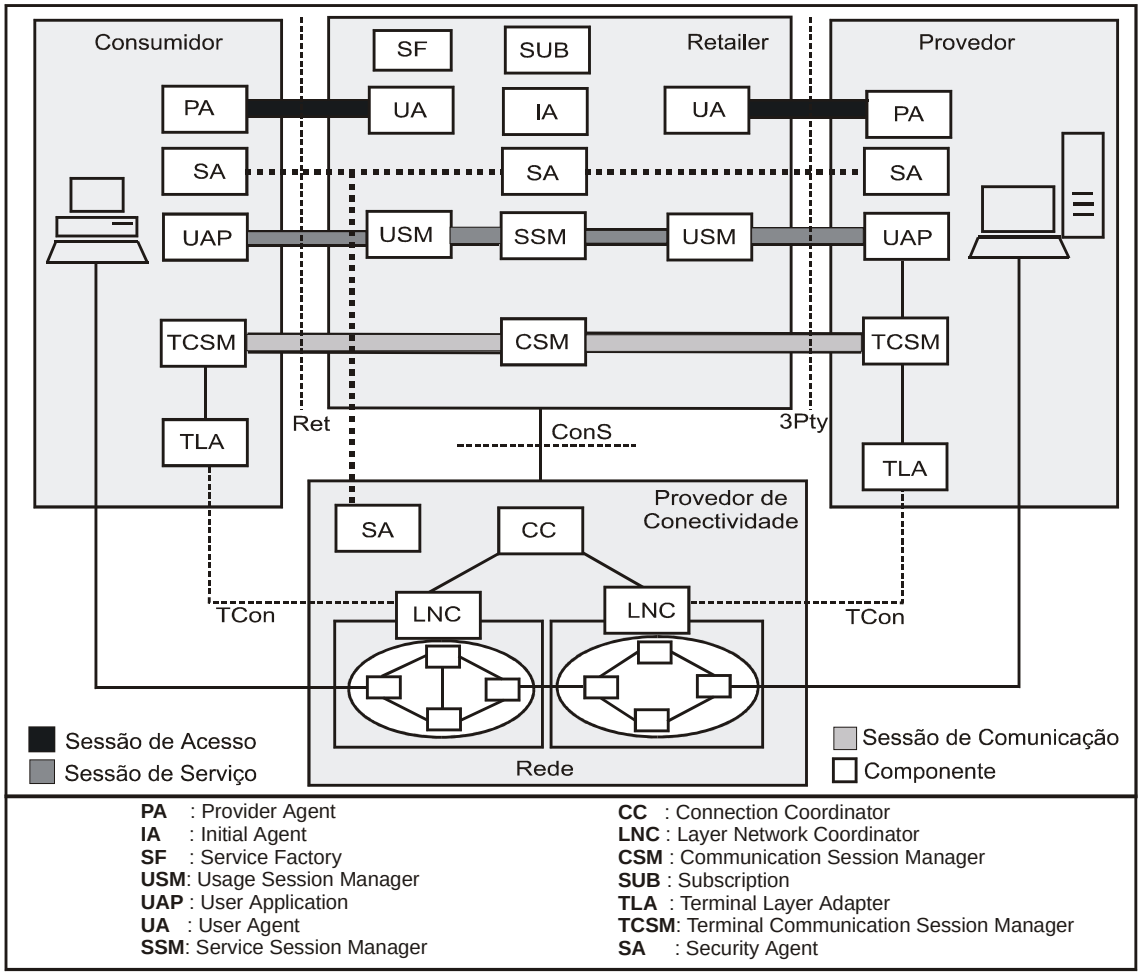

Figura 6-2: Visão geral da arquitetura de serviço (ABARCA, 1998).

a) Coletor de Eventos Contábeis

Este componente recebe, coleta e registra os eventos contábeis associados com o estado do Componente de Sessão ou com as mudanças de estado do Componente de Sessão. São registrados também eventos associados com a informação gerada pelo SSM (*Service Session Manager*). O Coletor de Eventos Contábeis é dividido em dois módulos: *EventMagememt* e *SessionComponent*.

b) Tarifação

Este componente é representado por dois módulos:
Módulo *Recovery*: permite fornecer a taxa de cobrança como uma função do estado do componente atual. Este converte os eventos contábeis coletados em registros de cobrança e armazena os mesmos dentro de uma base de dados. Em adição, ele permite restaurar a informação coletada quando ocorre uma falha no serviço.
Módulo *Tariff*: entrega a cobrança atual acumulada como uma função da seqüência de eventos. Este calcula a tarifa, usando a fórmula de cobrança de acordo com o contrato estabelecido e armazena as informações dentro de um registro *billing*.

c) Cobrança

Este componente pode ser automaticamente emitido ao final de um período negociado e definido no contrato com o cliente. Este componente é gerado através da informação de cobrança do registro *billing*. Existem quatro tipos de configurações *billing*: *On-line charging, Shared billing, Third-party billing* e *Credit-debit billing*. A implementação da cobrança na aplicação desenvolvida (protótipo) foi configurada de forma *on-line charging*.

d) Registro de Uso.

Durante o tempo de vida da conexão, este componente coleta e controla a aquisição de informações relacionadas com o uso dos recursos da rede gerados pelo LNC (*Layer Network Coordinator*). Este componente também registra os dados coletados para os processos futuros (gerenciamento de Falha e Desempenho).

6.2 Execução do Protótipo

Ao iniciar uma sessão, o usuário deve configurar as suas preferências de segurança que serão utilizadas na negociação para o estabelecimento da sessão.

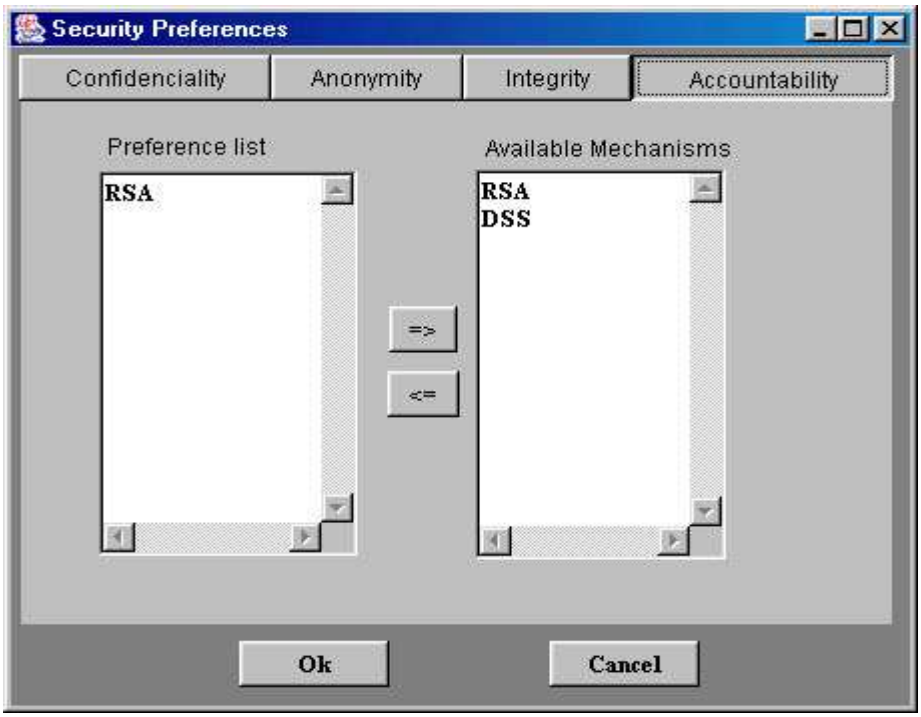

Figura 6-3 Caixa de diálogo para seleção de preferências de segurança.

A Figura 6-3 mostra a interface onde o usuário pode escolher quais objetivos de segurança ele irá usar e quais mecanismos existentes ele poderá usar para alcançar o objetivo de segurança desejado. Neste exemplo ilustrado, para se alcançar uma contabilidade eficiente, o usuário selecionou o algoritmo RSA.

Com as preferências do usuário já definidas, é verificada a necessidade de se fazer a negociação com o outro participante, caso seja necessário, a negociação ocorre como descrito na Figura 5-4.

Após a negociação ser concluída com sucesso, uma segunda interface é visualizada (Figura 6-1), subdividida nos seguintes módulos:

- ***Subscription*:** login do usuário e visualização dos dados do usuário;
- ***Update*** : atualização do usuário (*Insert, Modify, Delete, etc*);
- ***Monitoring service***: monitorização do serviço de vídeo conferência para cada usuário;

- ***Error messages***: visualização de erros que podem ocorrer durante a sessão de serviço.

O módulo cliente está divido em duas fases: fase de Inicialização e a fase de Monitoração.

a) fase de Inicialização

- O protótipo inicia um serviço quando é solicitado por um usuário (módulo *Service*, através do botão "*Start*" na Figura 6-1) que registra seu log, ingressando seu Id e password (módulo *Subscription* na Figura 6-1).
- Imediatamente, uma verificação (acesso à base de dados "*SubscripInfo.mdb*"). O usuário autorizado pode ser classificado em dois tipos:

  1. usuário "*com assinatura*", o qual tem um contrato com o provedor e sua prioridade no uso do serviço é completa: áudio (*fala-escuta*), vídeo (*visão-imagem*), por exemplo, A+V;

  2. usuário "*sem assinatura*", o qual usa o serviço pela primeira vez, não tem um contrato com o provedor, sua prioridade de uso do serviço é parcial e ele só assiste ao serviço: áudio (*escuta*), vídeo (*visão*), por exemplo, A. O novo usuário será registrado na base de dados (módulo *Update*: "*Add New User*" na Figura 6-1) para assegurar que sua quantidade de crédito disponível é suficiente para fazer uso do serviço ou de outra forma, dar um *log-out*, não permitindo o uso do serviço.

b) Fase de Monitoração

- Para cada usuário autorizado, seu próprio AcctMgmtCtxt é criado, iniciando o serviço (módulo *Service*, botão "*Enter*" na Figura 6-1).
- Automaticamente, o AcctMgmtCtxt cria os objetos (através das interfaces *SessionComponent* e *EventManagement*) que identificam os eventos gerenciados durante a execução.

Interface *SessionComponent*	**Interface *EventManagement***
{ SubscInfo SubsValid(in SubscInfor informacoes); ***Void*** AddNewUser(in SubscInfo informacoes); }	{***boolean*** RegService(in ***string*** cid, in ***long*** sertype); ***long*** GetTipoServico(in ***string*** cid, in ***long*** tipo_servico); ***long*** EnterEvent(in ***string*** csid, in ***long*** tipo_serv); ***long*** LeaveEvent(in ***string*** csid, in ***long*** tipo_serv); }

Ao mesmo tempo, um vetor de estado de sessão é gerado (SSVec) onde cada posição (pos) registra a informação relacionada aos eventos do serviço:

1. tempo inicial (ti);

2. tempo final (tf);

3. tempo acumulado pelo "*uso de serviço completo*": A+V (fs – full service) ou "*uso de serviço parcial*": (ps – partial service); e

4. tempo acumulado pelo "*uso de serviço compartilhado*" dos usuários (ts– time shared).

- Ao clicar no botão "*Enter*", o "ti" é inicializado enquanto "fs" ou "ps" são ativados. Como o vetor é visto como uma estrutura dinâmica e volátil, qualquer falha que ocorra durante o serviço é registrado como informação na base de dados. O *backup* é necessário para armazenar a informação (eventos) na base de dados ("*TariffInfo.mdb*") porque sua interação com o módulo Tariffing (interface *Tariff*) é periódica.

```
Interface Tariff
{  Tarval Tariff_val();  }
```

- Durante o período de serviço, o provedor deve estar verificando se o tempo consumido pelo usuário não excedeu 80% do tempo limite disponível. Se isto ocorrer, o provedor notifica ao usuário e o consulta se ele deseja aumentar a quota disponível (módulo *Update*: "*Change Max Amount*" na Figura 6-1), ou *log-out* do serviço (ativa a interface *Billing* para sua cobrança).

```
Interface Billing
{
  void BillingSave(in string cid, in string name, in string date, in long totalsecs, in long totalunits,
          in string inittime, in string endtime, in long asecs, in long avsecs, in long ssecs);
}
```

- O usuário que faz uso do serviço pode liberar a sessão (módulo *Service*, botão "*Leave*" na Figura 6-1). Nesse momento, o usuário entra no estado de áudio (A). Ele também tem a opção de retomar o serviço (módulo *Service*, botão "*Enter*" na Figura 6-1) ou finalizar a sessão (módulo *Service*, botão "*Stop*" na Figura 6-1).
- Existe também a opção de compartilhar o serviço entre vários usuários ao mesmo tempo. Isto acontece quando for ativado o botão "*Enter*" e então são disparados (inicializados) os temporizadores "ts" e para "fs" de cada usuário. Para liberar o estado de compartilhamento, é ativado o botão "*Leave*" para ativar "fs" ou o botão "*Stop*" para terminar a sessão.

- Se o usuário está no estado "*Stop*", os temporizadores são desativados, e "tf" é registrado. Finalmente, a cobrança *on-line* (interface *Billing*) é ativada pelos serviços fornecidos ao usuário e a informação é armazenada na base de dados "*BillingInfo.mdb*", (Figura 6-4).

Uma importante parte do serviço ocorre quando acontecem falhas. Por exemplo, eventos podem ser perdidos durante a sessão devido à perda da sincronização dos temporizadores. O estado contábil do SC pode ser interrompido por falhas na rede, falta de energia, etc. Nesse momento, a interface *Recovery* armazena e salva a informação na base de dados ("*TariffInfo.mdb*"). Se ocorrer uma falha e se o usuário desejar, a sessão é reiniciada e automaticamente se reinicializam os temporizadores para continuar a contabilização dos eventos, ou a sessão é encerrada. Para simular uma falha, clique "*X*" no canto superior direito da janela, e clique "*Start*" para continuar, como mostra a Figura 6-1.

```
Interface Recovery
{  boolean  CheckStatus (in string csid);  }
```

Na Figura 6-4 foram considerados na execução do protótipo três usuários que compartilham a mesma sessão de um "*serviço de vídeo conferência múltiplo*" fornecido pelo *Retailer*, mostrando um exemplo da interface gráfica "*Client*" com sua respectiva interface gráfica "*Billing*" que representa a cobrança on-line de um usuário pelo uso do serviço fornecido pelo *Retailer*.

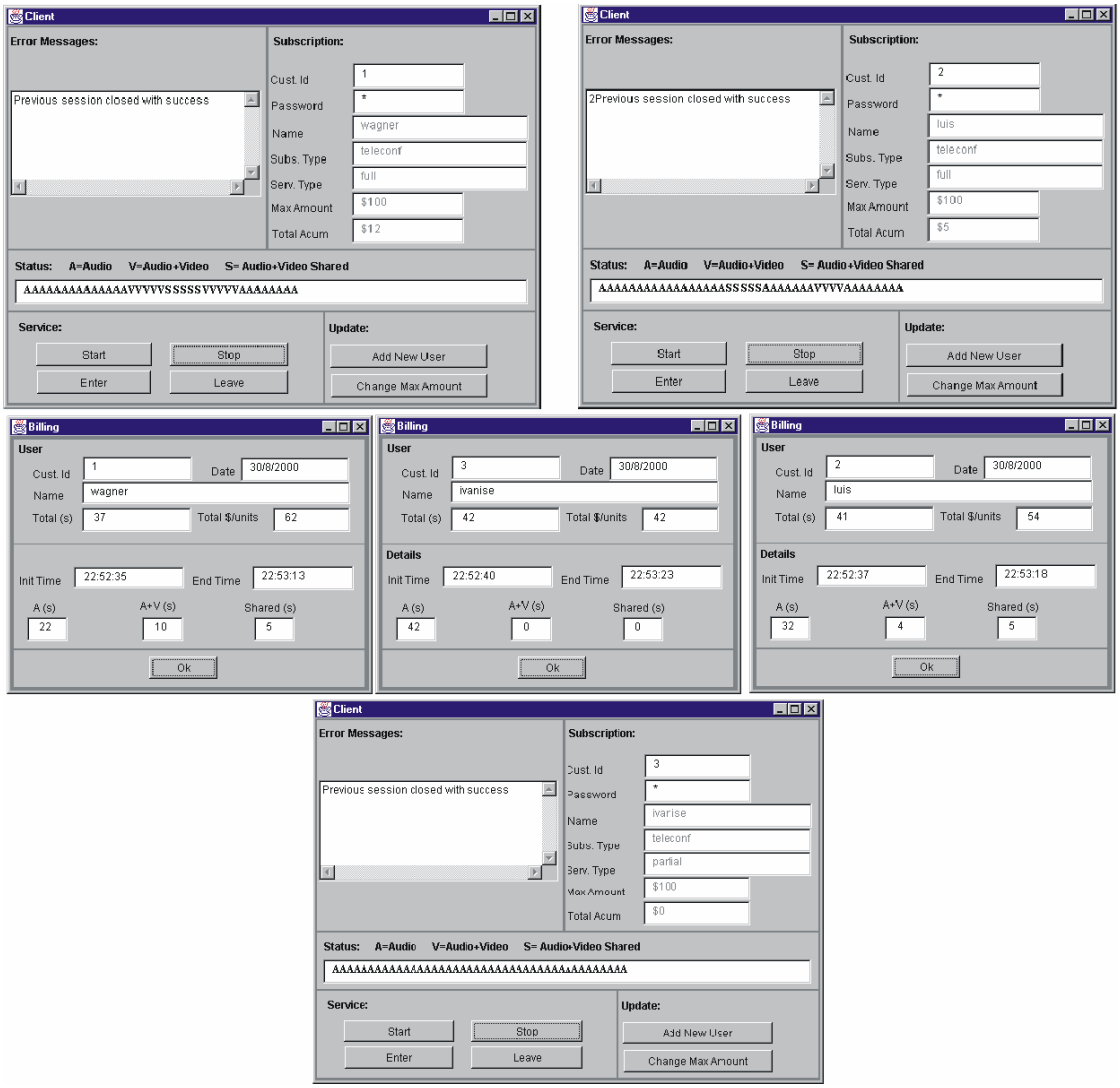

Figura 6-4: Exemplo de execução do Protótipo.

Os usuários tem três opções de acesso ao serviço de acordo ao contrato estabelecido entre as partes: V (Vídeo+Áudio); A (Áudio); e S (Vídeo+Áudio Compartilhado).

O uso da opção “V” custa 3$/unit, da opção “A” custa 1$/unit e da opção “S” custa 2$/unit.

6.3 Conclusão

Neste Capítulo foi apresentado os resultados obtidos com a implementação do modelo proposto, dando ênfase à negociação inicial entre os participantes e na execução do gerenciamento de contabilidade.

É importante destacar que, neste protótipo, todas as interfaces propostas pela arquitetura de serviço TINA foram criadas, mas somente as interfaces que possuíam aderência com

o assunto de tarifação, eventos contábeis e segurança foram implementadas. Outras interfaces com a de recuperação (*recovery*) não foram implementadas visto que não pertencem ao objetivo deste trabalho.
A seguir será apresentado as conclusões finais e trabalhos futuros.

6. Conclusões e Perspectivas Futuras

Os esforços empreendidos pelo consórcio TINA-C resultaram em uma arquitetura repleta de detalhes e ricamente documentada, permitindo um claro entendimento do problema no que concerne à gerência de segurança e a gerência de contabilidade.
Através desta mesma documentação, ficou evidente que as deficiências tratadas neste trabalho não foram produto de imprudência dos idealizados da arquitetura TINA, mas sim devido ao fato de que estas deficiências não existiam no ambiente que precede ao proposto pelo consórcio, isto é, até o momento da criação da arquitetura TINA, boa parte dos integrantes do consórcio eram empresas de telecomunicações onde todos se conheciam e possuíam um certo grau de confiança entre eles. Com a proposta de uma natureza aberta de TINA (onde novos atores surgiram, inclusive o usuário final), e, somado com os problemas associados aos sistemas distribuídos, os riscos de ataques e problemas de segurança se tornam ainda maiores e evidentes.
O principal objetivo desde trabalho foi de explorar a gerência de segurança no âmbito da gerência de contabilidade TINA. Como resultado, levando-se em consideração o modelo da arquitetura já existente, um modelo foi estruturado e um protótipo implementado para validar este modelo proposto.
As facilidades e os serviços da CORBA oferecem um conjunto de interfaces que permitem a construção da gerência do serviço da TINA. Este trabalho fornece uma visão geral dos conceitos TINA que especifica o contexto da gerência de contabilidade. São descritas as características da contabilidade, requisitos e algumas questões da gerência de contabilidade.
Desse modo, é proposta uma arquitetura de gerência de contabilidade especificando um modelo arquitetural que contêm componentes específicos tais como AcctMgmtCtxt,

Componente de Sessão, etc, que abrange diferentes aspectos do controle e gerenciamento de serviço.

6.1 Trabalhos futuros

Durante a execução deste trabalho, além de explorar os problemas na gerência de segurança e na gerência de contabilidade, percebeu-se também uma grande deficiência na porção referente à gerência de falhas. Apesar de citado e tratado como importante, poucas informações sobre a gerência de falhas foram encontradas, tornando a gerência de falhas um importante assunto para trabalhos futuros.

Na arquitetura TINA ainda existem diversas áreas onde a Qualidade de Serviço (*QoS*) poderia ser utilizadas com consideráveis ganhos no serviço oferecido. Complementando os conceitos de Qualidade de Serviço, conceitos de Acordo em Nível de Serviço (*SLA*) com certeza se mostra uma área promissora para pesquisas e desenvolvimentos.

Tratando de assuntos afins a este trabalho, a concepção de um Servidor de Segurança ao modelo, aos moldes de instituições certificadoras, também se qualifica como um tema interessante a ser pesquisado.

Não se pode descartar em trabalho futuro a implementação de todo o modelo proposto pelo consórcio TINA. Neste trabalho, o protótipo foi desenvolvido utilizando-se a implementação do CORBA provida pelo Visibroker. Como a arquitetura TINE propõe o uso de uma DPE independente de implementações específicas, o uso de outros ORBs irá possibilitar a experiência em ambientes heterogêneos além de permitir um *benchmarking* com o DPE utilizado neste trabalho.

8. Bibliografia

(ANDERSON, 1998) ANDERSON, R. et al ***The Steganographic File System.*** Cambridge University. [www.cl.cam.ac.uk/ftp/users/rja14/sfs3.pdf] ,1998.

(ABARCA, 1997) ABARCA, C.; et al. ***Network Resource Architecture***, v. 3.0, TINA-C, [http://www.tinac.com], 1997.

(ABARCA, 1998) ABARCA, C.; et al. ***Service Component Specification Computational Models and Dynamics***, v. 1.0b, TINA-C, [http://www.tinac.com], 1998.

(BLEUMER, 2000) BLEUMER, G. ***Biometric Authentication and Multilateral Security*** In: Multilateral Security in Communications, Stuttgart, Alemanha. 1999.

(BRENNAN, 2000) BRENNAN, R. et al. ***Evolutionary Trends in Intelligent Networks***, In: IEEE Communications Magazine, Junho 2000 – págs 86-93

(BRINKSMA, 1988) BRINKSMA, E. ***A tutorial on LOTOS***, ISO8807 Information Processing Systems – Open Systems Interconnection – LOTOS - A formal description technique based on the temporal ordering of observational behaviour, 1988.

(BUTTYÁN, 1999) BUTTYÁN, L. et al ***Multilateral Security in Middleware-Based Telecommunication Architectures*** In: Multilateral Security for Global Communication, Addison-Wesley, 1999.

(CADP, 1999) CADP. ***Caesar/Aldebaran Development Package,*** [http://www.inrialpes.fr/vasy/cadp.html], 1999.

(CLAUB, 2001) CLAUB, S. et al. ***Identity management and its support of multilateral security***. Computer Networks 37, páginas 205-219, 2001.

(FARLEY, 1998) FARLEY, P.; et al. ***Ret Reference Point Specification***, v. 1.0, TINA-C, [http://www.tinac.com], 1998.

(HAMADA, 1996) HAMADA, T, et al ***Accounting Management Architecture,*** TINA-C, [http://www.tinac.com], 1996.

(HELLEMANS, 1997) HELLEMANS, P. Et al ***TINA Service Architecture: From Specification to Implementation*** In: TINA ´97 – Global Convergence of Telecommunication and Distributed Object Computing, 1997

(IETF,1999) IETF. ***The PINT Service Protocol: Extensions to SIP and SDP for IP Access to Telephone Call Services,*** draft-ietf-pint-protocol-01, [http://www.bell-labs.com/mailing-lists/pint/], 1999

(ISO, 1994) ISO/IEC 10764 / ITU-T X.900, ***Information Processing – Open Distributed Processing – Basic Reference Model of ODP – Part 1: Overview and Guide to Use***, 1994.

(ITU, 1993) ITU-T M.3010. ***Principles for a Tellecomunication Management Newtwork.*** 1993.

(KRISTIANSEN, 1997) KRISTIANSEN, L. et al ***TINA Service Architecture 5.0*** , TINA-C, [http://www.tinac.com], 1997.

(MULDER, 1997) MULDER, H. et al ***TINA Business Model and Reference Points,*** TINA-C, [http://www.tinac.com], 1997.

(NIEHAUS, 1999) NIEHAUS, D. ***Telecommunications Information Networking Architecture***. In: ITTC – Information and Telecommunication Technology Center, University of Kansas. [http://hegel.ittc.ukans.edu/projects/tina-c] 19/09/2001.

(NISHIKAWA, 1997) NISHIKAWA, H. et al , ***Data-Driven Implementation of TINA kernel Transport Network*** In: TINA ´97 – Global Convergence of Telecommunication and

Distributed Object Computing, 1997 (83350184.pdf)

(NOTARE, 2000) NOTARE, M.S.M.A. ***Concepção, Desenvolvimento e Análise de um Sistema de Gerência de Segurança para Redes de Telecomunicações.*** Florianópolis, 2000. Tese de Doutorado (Programa de Pós-Graduação em Ciência da Computação). Laboratório de Redes e Gerência, Universidade Federal de Santa Catarina.

(PARLAY,2001) PARLAY. ***Open Service Access: Application Programming Interface,*** V1.1.1 ,The Parlay Group, [http://www.parlay.org], 2001.

(PAVLOU,1998) PAVLOU, G. et al. ***An evolutionary approach towards the future integration of IN and TMN,*** In: Interoperable Communications Networks 1, 1998

(PFITZMANN, 2001) PFITZMANN, A. ***Multilateral Security: Enabling Technologies and Their Evaluation***. In: Informatics: 10 Years Back. 10 Years Ahead, LNCS 2001

(PFITZMANN, 1998) PFITZMANN, A. et al ***A Java-based distributed platform for multilateral security*** In: Lectures Notes in Computer Science, 1998.

(PFITZMANN, 2002) PFITZMANN, A. et al. ***Striking a Balanc between Cyber-Crime Prevention and Privacy.*** IPTS-Institute for Prospective Technological Studies- Report vol. 57, 2002

(RANNENBERG, 2000) RANNENBERG, K. ***Multilateral Security – A concept and examples for balanced security.*** In: New Security Paradigms Workshop 2000. Irland, 2000.

(SAILER, 1998) SAILER, R. ***An Evolutionary Approach to Multilaterally Secure Services in ISDN/IN*** In: Seventh International Conference on Computer Communications and Networks, Louisiana, 1998. páginas 276-283.

(SAILER, 1999) SAILER, R. et al ***Security Functions in Telecommunications – Placement & Achievable Security.*** In: Multilateral Security in Communications, Addison-Wesley-Longman, 1999. páginas 323-348.

(SEKKAKI, 2001a) SEKKAKI, A et al ***Security within TINA Accounting Architecture Management"*** In: ICC2001 International Conference on Communications, Helsinki – Finlândia, 2001.

(SEKKAKI, 2001) SEKKAKI, A. et al. ***Development of a Prototype Based on TINA Accounting Management Architecture*** In: IFIP/IEEE International Simposium on Integrated Network Management. , 2001. v.1. p.100 - 120

(STAAMANN, 1997) STAAMANN, S. et al. ***Security in the Telecommunications Information Networking Architecture – the CrysTINA Approach.*** In: TINA 97 – Global Convergence of Telecommunications and Distributed Object Computing , 1997. IEEE

(TINA, 2000) TINA, ***About TINA-C,*** [http://www.tinac.com/about/about.htm], 2000